Habilitation à Diriger des Recherches

Université Paris 8, Département de Mathématiques

Laboratoire Analyse, Géométrie et Applications (LAGA), Université Paris 13 et Université Paris 8, UMR 7539, CNRS

Équipe Mathématiques pour le traitement de l'information et de l'image (MTII)

Spécialité : Mathématiques

Sihem Mesnager

10 décembre 2012

Contributions aux fonctions booléennes pour la cryptographie symétrique et aux codes correcteurs d'erreurs

HABILITATION

Jury

Mme. Pascale CHARPIN, Directrice de Recherche, INRIA-Rocquencourt, France	Rapporteure
M. Tom HØHOLDT, Professeur, Université de Copenhague, Danemark	Rapporteur
M. Matthew Geoffrey PARKER, Professeur, Université de Bergen, Norvège	Rapporteur
Mme. Anne CANTEAUT, Directrice de Recherche, INRIA-Rocquencourt, France	Examinatrice
M. Claude CARLET, Professeur, Université de Paris 8, France	Examinateur
M. Gérard D. COHEN, Professeur, Télécom ParisTech, France	Examinateur

Université Paris 8
Département de mathématiques
Ecole Doctorale Sciences CLI
2, rue de la liberté — 93526 Saint-Denis — Tél. + 33 (0)1 49 40 64 20 — http ://www.univ-paris8.fr/

Contributions on Boolean functions for Symmetric Cryptography and Error-Correcting Codes

(This manuscript is dedicated to the memory of Philippe Flajolet[1])

Sihem MESNAGER

[1] Philippe Flajolet was a great mathematician and computer scientist. Although Philippe has not worked in my field, he was very curious about my research area during our scientific discussions. It was a real pleasure to exchange ideas with him during our joint ANR Boole meetings. I'll always remember his human qualities and stimulating mathematical discussions.

et à maman chérie

Abstract

In this manuscript are presented our results about Boolean functions and Coding theory. Our main contributions are on bent functions, hyper-bent functions and the covering radii of Reed-Muller codes.

Our main contribution about bent functions is to extend a class proposed by Dillon, in which he did not succeed in exhibiting new bent functions. That extension can be linked to a classical family of polynomials in finite projective geometry, the o-polynomials. That allows us to establish a relationship between classes of bent Boolean functions and geometric objects: hyperovals. That link leads to many potentially new families of bent functions, especially new Niho bent functions. It also offers a new framework to study Niho bent functions and to compute their dual functions.

In the line of Charpin, Dillon and Gong we have found, the first non monomial families of hyper-bent functions. Notably Dillon (1974) has linked zeros of Kloosterman sums to monomial bent functions. In the same vein, we establish a link between the value 4 of Kloosterman sums and non monomial bent functions. We extend that result to many others families characterizing the hyper-bent elements by means of exponential sums involving Dickson polynomials (and more efficiently by means of cardinalities of hyperelliptic curves).

In Coding theory, the most important result is to have significantly improved the upper bounds (dating from 15 years ago) on the covering radii of Reed-Muller codes of orders greater than 1. That results has been obtained thanks to character sums and the analysis of the structure of codewords of low weights of the dual of the Reed-Muller code of order 2.

Résumé

Dans ce manuscrit sont présentés nos principaux travaux sur les fonctions booléennes et en théorie des codes. Nos avancées les plus importantes portent sur les fonctions courbes, les fonctions hyper-courbes et le rayon de recouvrement des codes de Reed-Muller.

Sur les fonctions courbes, la principale contribution est une extension d'une classe de fonctions courbes proposée par Dillon dans laquelle il n'avait pas reussi à exhiber de nouvelles fonctions courbes. Le principal apport de cette extension est que les fonctions courbes de cette nouvelle famille peuvent être reliées avec des polynômes connus et étudiés en géométrie projective discrète : les o-polynômes. Cela conduit à un lien entre les fonctions booléennes courbes et des objets géométriques : les hyper-ovales. Ce lien permet d'obtenir plusieurs familles de fonctions courbes potentiellement nouvelles. En outre, cette extension permet de générer de nouvelles fonctions courbes de type Niho et d'offrir un nouvel angle d'attaque pour calculer les duales des fonctions courbes de Niho.

Dans la continuité des travaux de Charpin, Dillon et Gong, nous avons obtenu les premières familles infinies non monomiales de fonctions hyper-courbes. En particulier, Dillon (1974) avait montré comment construire à partir des zéros des sommes de Kloosterman des fonctions monomiales courbes. Dans la même veine, nous établissons un lien entre la valeur 4 de la somme de Kloosterman et des fonctions non monomiales courbes. Nous étendons ensuite ce résultat et et caractérisons au moyen de sommes exponentielles et des polynômes de Dickson les éléments hyper-courbes de plusieurs familles de fonctions booléennes (et même efficacement au moyen de cardinaux de courbes hyperelliptiques).

En théorie des codes, le résultat le plus important est d'avoir réussi à améliorér les bornes supérieures (vieilles de plus de 15 ans) sur le rayon de recouvrement des codes de Reed-Muller d'ordres strictement supérieurs à 1. Ce succès a été obtenu au moyen de sommes de caractères et grâce à l'analyse de la structure des mots de poids faibles du dual du code de Reed-Muller d'ordre 2.

Contents

List of figures

List of tables

List of algorithms

List of symbols and notation

General

$\#S$	Cardinality of the set S	xxi
$\mathbb{C}$	Field of complex numbers	xxi
$\mathbb{F}_{2^n}$	Finite field with 2^n elements	xxi
$\mathbb{F}_q$	Finite field with q elements	xxi
$\overline{K}$	An algebraic closure of K	xxi
$\mathbb{R}$	Field of real numbers	xxi
$\mathbb{N}$	Semiring of non-negative integers	xxi
$\oint$	Cauchy integral	72
$\mathbb{F}_2^n$	The vectorspace of all binary vectors of length n	xxi
$\mathbb{Z}$	Ring of integers	xxi
$G_K(z)$	The multivariate generating function associated to z	72
K, L	A perfet field or a number field	xxi
l	A prime number different from p	xxi
p	A prime number	xxi
q	A prime number's power	xxi

Combinatorics

$\binom{n}{k}$	Binomial coefficient	8

Boolean functions

$AI(f)$	Algebraic immunity of f	61
χ_f	The sign function of a Boolean function f	41
$\mathcal{RM}(r, n)$	Reed-Muller code of order r and length 2^n	104
Res_n^m	The set of all n-variable m-resilient Boolean functions	70

$\mathcal{PS}$	Partial Spread class	106
$\mathfrak{S}_n^m$		73
$\mathfrak{F}_n$	The set of functions $f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$	157
$\mathfrak{G}_n$	The set of functions $g_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$	171
$\mathfrak{H}_n$	The set of functions $f_{a_r,b}(x) := \sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$	182
$\mathfrak{W}_n$	The set of functions $f_{a,b}(x) := \sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$	194
$\mathcal{PS}_{ap}^{\#}$	Class $\mathcal{PS}_{ap}^{\#}$	155
Θ_n^m	The subset of $\mathcal{P}_n$ of all subsets whose cardinality is at most $n-m-1$	70
$PG_2(2^n)$	The projective space of dimension 2 over finite field $\mathbb{F}_q$	139
$PG_n(q)$	The projective space of dimension n over $\mathbb{F}_{2^n}$	139
$\mathcal{B}_n$	The set of all Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$	37
$\mathcal{M}$	Maiorana-McFarland class	106

Finite fields and Exponential sums

$\mathcal{T}_i$		44
$\mathrm{Tr}_r^k(\cdot)$	The trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$	39
$\mathrm{Tr}_1^n(\cdot)$	The absolute trace: trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$	39
$\widehat{\chi_f}(\omega, k)$	The extended Walsh-Hadamard transform ($\omega \in \mathbb{F}_{2^n}$, k an integer co-prime with 2^n-1)	42
$\Xi(f)$	The exponential sum associated with f	44
$C_m(a,b)$	The binary cubic sums on $\mathbb{F}_{2^m}$ associate with a and b	43
$D_r(X)$	Binary Dickson polynomial of degree r	53
$K_m(a)$	The Binary Kloosterman sums on $\mathbb{F}_{2^m}$ associate with a	42
$T_i(f)$	The partial exponential sum on $\mathcal{T}_i$ associate with f	44
U	The cyclic group of 2^m+1-st roots of unity in $\mathbb{F}_{2^n}$	45

Overview

The manuscript is split into two parts even if there is a link between the two parties. The first part is composed of 9 chapters. In each chapter (except Chapter 1), we first begin by some preliminaries providing enough background for the unfamiliar reader to understand the contents of the chapter in which we present advanced results and the contribution of the author to the subject. The second part is dealing with the covering radius of Reed-Muller codes.

A notation list can be found on Page xix, before the table of contents. In the following, we summarize the contains of each chapter as well as our main contribution and the references of the published papers. In each chapter, we shall give the technical details and proofs of our results (which have already been published, except Section 6.4, Section 6.5 and Section 6.6 of Chapter 6 and Subsection 7.3.4 of Chapter 7 which are extended the part of [202]). For the results of other authors, the reader may refer to the corresponding reference.

0.1 Chapter 1

In Chapter 1 we briefly present some generalities on Boolean functions including some of their different representations used in the whole the manuscript.

0.2 Chapter 2

0.2.1 Summary of the main contributions

We provide several technical results and some mathematical tools that we need subsequently in Chapter 5, Chapter 7 and Chapter 8. More precisely, firstly, we are interested to express some particular exponential sums over the unit circle in $\mathbb{F}_{2^n}$ (that is, the cyclic group of 2^m+1 st roots of unity in $\mathbb{F}_{2^n}$) by means of Kloosterman sums and cubic sums. Such expressions will be used to exhibit conditions of bentness and semi-bentness (of some Boolean functions in polynomial forms) involving Kloosterman sums and cubic sums. Secondly, we study the action of Dickson polynomials on subsets of finite fields of even characteristic related to the trace of the inverse of an element and provide an alternate proof of a not so well-known result. Such properties are then applied to the study of families of Boolean functions and characterizations of their hyper-bentness in terms of exponential sums.

0.2.2 Publications

The results presented in this chapter constitute some excerpts from the following references:

- S. Mesnager. A new family of hyper-bent Boolean functions in polynomial form. Proceedings of Twelfth International Conference on Cryptography and Coding. Cirencester, United

Kingdom. M. G. Parker (Ed.) IMACC 2009, LNCS 5921, Springer, pages 402–417, 2009 ([196]).

- S. Mesnager. Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. IEEE Transactions on Information Theory-IT, Vol 57, No 11, pages 744–7458, 2011 ([199]).
- J-P Flori and S. Mesnager. Dickson polynomials, hyperelliptic curves and hyper-bent functions, Proceedings of 7th International conference SEquences and Their Applications SETA 2012, LNCS 7280, Springer, pages 40–52, 2012 ([102]).

0.3 Chapter 3

Boolean functions, that is, $\mathbb{F}_2$-valued functions defined over the vector space $\mathbb{F}_2^n$ of all binary vectors of a given length n, are used in the S-boxes of block ciphers and in the pseudo-random generators of stream ciphers. They are very important primitives of symmetric cryptosystems and play a central role in their security. In stream ciphers, the main model for the generation of the keystream consists of a linear part, producing a sequence with a large period, usually composed of one or several LFSRs, and a nonlinear combining or filtering function f which produces the output, given the state of the linear part. In the nonlinear combiner sub-model, the outputs to several LFSRs are combined using a nonlinear Boolean function to produce the keystream. In the nonlinear filter sub-model, the content of some of the flip-flops in a single (longer) LFSR constitute the input to a nonlinear Boolean function which produces the keystream. These models which are very efficient, in particular in hardware, have undergone a lot of cryptanalysis and to resist those attacks, different design criteria have been proposed for both the LFSRs and the combining Boolean function. Obviously, the properties of such functions are critical for the security requirements of the final system built upon them. If not carefully chosen, the use of a *weak* Boolean function can indeed jeopardize the entire system. Therefore, several *cryptographic properties* have been defined and studied to ensure immunity of the system to different kinds of attacks; the ever evolving design of those naturally entails new restrictions on the classes of eligible Boolean functions, so that they become narrower and narrower and their constructions, or even their characterizations, become harder and harder.

At the beginning of Chapter 3, we survey the main cryptographic criteria for designing the (cryptographic) Boolean functions. Note that some of these notions are muturally *incompatible* and *trade-offs* have to be made to meet as many *criteria* as possible. The corresponding attacks will also be mentioned, but not thoroughly described. For a more classical and deeper exposition we refer the reader to Carlet's chapter ([31], Chapter 8).

0.3.1 Summary of the main contributions

In this chapter, our contributions were in the following topics which fall within the cryptographic framework of Boolean functions:

1- Immunity profile of Boolean function:
The combining function must be balanced for the good statistical properties of the generated stream sequence. Moreover, to avoid a divide and conquer attack (see *e.g.*[22, 251, 187, 236]), the combining function must avoid low order correlation . This is the reason why such a combining function is often chosen with a rather high correlation immunity order.

There are two equivalent ways for characterising the correlation immunity: either by means of the Walsh transform or by means of the sub-functions. Originally, an n-variable Boolean function f is said to be *correlation immune* of order t (or t-th order correlation immune) if any sub-function deduced from f by fixing at most t inputs has the same output distribution as f. On the other hand, correlation immunity can be characterised by means of the Walsh transform of f : $\widehat{\chi_f}(\omega) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+\omega\cdot x}$ (that is, the Fourier transform of the sign function $\chi_f(x) = (-1)^{f(x)}$). A Boolean function f is correlation immune of order t if and only if the Walsh transform of f vanishes at every non zero vector of Hamming weight at most t [266]. If f is moreover balanced, then f is said to be t-resilient.

Siegenthaler's bound [236] states that the algebraic degree of an n-variable t-th order correlation immune Boolean function is necessarily less than or equal to $n - t$ [236]. On the other hand, the nonlinearity of a t-th order correlation immune Boolean function is necessarily less than or equal to $2^{n-1} - 2^t$ if $t > \frac{n}{2} - 1$ and $2^{n-1} - 2^{\frac{n}{2}-1} - 2^t$ (if n even) otherwise [46]. When the Boolean function is moreover balanced, the upper bounds on its algebraic degree and its nonlinearity are lower. Indeed, the algebraic degree is less than or equal to $n - t - 1$ and the nonlinearity is upper bounded by $2^{n-1} - 2^{t+1}$ if $\frac{n}{2} - 1 < t < n - 1$ and $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{t+1}$ if $t \leq \frac{n}{2} - 1$ (n even). Therefore, the correlation immunity criterion is not compatible with an high algebraic degree (necessary to withstand Berlekamp-Massey attack) and a high nonlinearity (necessary for avoiding attacks using linear approximation of the function). Moreover, the recent algebraic attacks, *e.g* [72, 73], highlighted the need for having an high algebraic degree as well as an high algebraic immunity so that stream ciphers can resist to these attacks. Now, there seems to be some kind of contradiction for Boolean functions between having high correlation immunity and optimum or nearly optimum algebraic immunity; also, much attention having been given to algebraic immunity recently, several examples of functions having optimum algebraic immunity could be found but no example of correlation immune Boolean function of order larger than 1 with optimum algebraic immunity.

Fortunately, as observed by Kurosawa and Matsumoto ([155]), strict correlation immunity is not absolutely required. The work factor to reconstitute the sequences coming from several registers increases with the number of registers, and a strict correlation immunity is necessary for small orders only. For higher orders, low non-zero correlations are sufficient (the lower the order, the lower the allowed correlations). In [155], the notion of resilient function has been weakened to match more properly the features required for Boolean functions used in stream ciphers. The resiliency constraints have been relaxed by introducing the notion of *almost-resiliency*, that amounts to saying that the values of the Walsh transform is upper bounded on all vectors of weight lower than some positive integer. Kurosawa and Matsumoto allow the restrictions to have output distributions slightly differing from the distribution of the global function.

On our side, we have proposed an alternate way of relaxing the constraint of correlation immunity. We have allowed the Walsh transform to take low values for low orders instead of being null. We have introduced the new concept of *immunity profile* of a Boolean function:

Definition 0.3.1. *Let n be any integer, $n \geq 2$. Let φ be any integer valued mapping over the set $\{0, \ldots, n\}$. A Boolean function f over $\mathbb{F}_2^n$ is said to be φ-correlation immune if, for any vector $\omega \in \mathbb{F}_2^n$,*

$$|\widehat{\chi_f}(\omega)| \leq \varphi(\mathrm{wt}(\omega))$$

where $\mathrm{wt}(\omega)$ denotes the Hamming weight of vector ω which is by definition the number of non zero components. If f is moreover balanced then f is said to be φ-resilient. The integer mapping

φ is called the immunity profile *of f.*

Our definition generalizes correlation immunity as t-th order correlation immune Boolean functions are φ-correlation immune with $\varphi(i) = 0$ for $1 \leq i \leq t$ and $\varphi(i) = 2^n$ for $i \geq t+1$ or $i = 0$. Every Boolean function is clearly φ-correlation immune for some φ. It is advisable to carefully choose the integer mapping φ. It seems natural to consider increasing mappings φ, which take low values for low orders. Because of Parseval's identity, the immunity profile φ of f must satisfy

$$\sum_{l=0}^{n} \binom{n}{l} \varphi^2(l) \geq 2^{2n}.$$

We have studied the notion of φ-correlation immune and provided a way to transfer this notion for n-variable Boolean functions to sub-functions ($(n-r)$-variable Boolean functions) :

Proposition 0.3.2. *Let $f \in \mathcal{B}_n$ and let φ be any integer-valued mapping over $\{0, \ldots, n\}$. For any subset $I = \{i_1, \ldots, i_r\}$ of $\{1, \ldots, n\}$, we denote by f_I^σ the sub-function on $\mathbb{F}_2^{n-r}$ obtained by setting the i_jth input to σ_j for every $j \in \{1, \ldots, r\}$. Assume that f is φ-correlation immune. Let $r \in \{1, \ldots, n-1\}$, $\sigma \in \mathbb{F}_2^r$ and $\{i_1, \ldots, i_r\} \subset \{1, \ldots, n\}$.*
Then f_I^σ is φ_r-correlation immune with $\varphi_r(k) = \frac{1}{2^r} \sum_{j=0}^{r} \binom{r}{j} \varphi(k+j)$, $k \in \{0, \ldots, n-r\}$.

We have studied the alternate notion of almost resilient function and we have seen that both definitions go in the same direction, but with non-negligible differences. We have seen that the notion that we have introduced is slightly more general as we are interested in the whole profile and in a way which sticks more precisely to the effective difficulty of the correlation attack. We have studied the relationship between the immunity profile and the approach of almost resiliency introduced by Kurosawa and Matsumoto. We have proved the following connection between the two notions:

Proposition 0.3.3. *Let n be any integer, $n \geq 2$. Let φ be any integer-valued mapping over the set $\{1, \ldots, n\}$. Let f be a Boolean function over $\mathbb{F}_2^n$. Assume that f is φ-correlation immune. Then f is $\varepsilon_{\varphi,t}$-almost $(n, 1, t)$ resilient for any positive integer t less than n where $\varepsilon_{\varphi,t} = \frac{1}{2^{n+1}} \sum_{j=1}^{t} \binom{t}{j} \varphi(j)$.*

Moreover we wondered which immunity profile should have the combining Boolean function to have a good resistance to fast correlation attacks [22, 251]. Fast correlation attacks model the combining function as a noise on a communication channel and the cryptanalysis as a decoding problem of the keystream. There are then two ways of making hard the task of the cryptanalyst: either to oblige him to have a very large amount of the keystream or make the decoding step having a too high complexity. By considering these two points of view separately, we find two possible types of immunity profile: with arguments taken from the information theory, we explain that the immunity profile could increase in proportion to the square root of the order; next, considering the complexities of the decoding procedures used in fast correlation attacks, we have seen that the combining Boolean function could have an exponential immunity profile. Next, we have considered another class of ciphers that are iterated ciphers (for example, self synchronizing stream ciphers). We explain that in this kind of cipher, a round ciphering function with an exponential immunity profile may provide a better resistance to linear cryptanalysis.

Finally, we have proposed two primary constructions and two secondary constructions of φ-correlation immune Boolean functions. For the primary constructions, we have showed that one can design ψ-correlation immune Boolean functions from the class of Maiorana-McFarland with $\psi(i) = \lambda 2^r \varphi(\min(i, r))$ for $i \in \{0, \ldots, n\}$ provided that $\lambda \sum_{l=0}^{r} \binom{r}{l} \varphi(\ell) \geq 2^s$ under the assumption

$\#\pi^{-1}(a) \leq \lambda\varphi(\mathrm{wt}(a))$ for every $a \in \mathbb{F}_2^r$. We have also proposed symmetric Boolean functions with exponential correlation immunity profile using the Krawtchouk polynomials.

To conclude, we have introduced a new concept of immunity profile leading to a notion of φ-correlation immunity for relaxing the constraint of correlation immunity. We have studied an alternative notion of almost resilient function. We have showed that our concept corresponds more closely to the requirements that make the cipher more resistant to precise attacks and proposed primary and secondary constructions with the selected profile.

2- On the number of resilient Boolean functions:
To increase the security of symmetric cryptopsystems, Boolean functions have to fit several security criteria. It is important to ensure that the selected criteria for the Boolean functions, supposed to be used in some cryptosystems, do not restrict the choice of fonction too severely that is, the set of functions must be enumerated. Cryptographic functions needing to satisfy specific criteria. Having specific criteria, it is important to know if there exist sufficiently large numbers of functions satisfying them. As a result the problem arises of enumerating sets of functions satisfying various criteria or even (as a starting point) satisfying one criterion. But even such simplified enumeration is unknown for most criteria.

Among all the security criteria, two crucial criteria are: the Boolean function has be balanced, that is takes the value 1 with probability 1, and m-correlation immune, that is, the output distribution does not change if we fix at most m inputs. The Boolean functions that are both balanced and m-correlation immune are said to be m-resilient. The literature about correlation immune or resilient Boolean functions is very rich and a lot of problems on this subject remain open. Notably, the problem of counting the size of the set of m-resilient n-variable Boolean functions (denoted by Res_n^m) is still challenging. Indeed, this number is only known for $m = 1$ up to 7 variables (the number of 1-resilient 7-variable Boolean function have been found in 2007 [3]) and for $m \geq n - 3$ for every n [17]. This problem seems to be untractable. In 2010, Canfield et al.[18] have obtained an asymptotic estimatimation of the number of n-variable m correlation immune Boolean functions.

Our approach for the problem of counting the number of m-resilient n-variable Boolean functions was to use the numerical normal form[2] of Boolean functions of to reword the problem of counting the number of m-resilient n-variable Boolean functions in that to count the number of integer solutions of a system of linear inequalities:

Proposition 0.3.4. *Let $\mathfrak{R}_n^m$ be the subset of $\mathbb{R}^{\Theta_n^m}$ defined as*

$$\mathfrak{R}_n^m = \Big\{ (x_J)_{J\in\Theta_n^m} \in \mathbb{R}^{\Theta_n^m} \;\Big|\; \forall I \in \mathcal{P}_n,\, 0 \leq \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J \leq 1 \Big\}. \tag{1}$$

Then,

$$\#Res_n^m = \#(\mathbb{Z}^{\Theta_n^m} \cap \mathfrak{R}_n^m).$$

We then use a classical approach of enumerative combinatorics to count integer solutions of linear systems with integer coefficients, that is, we introduce a multivariate generating function and express the number of m-resilient n-variable Boolean functions with respect to the coefficients of this multivariate generating function. We then use multivariate residue calculus to derive a representation formula by means of the Cauchy integral:

[2]Notion introduced by Carlet and Guillot (see [38, 39])

Proposition 0.3.5. *We have*

$$\#Res_n^m = \frac{1}{(2i\pi)^{2^n}} \oint G(z)\frac{dz}{z} \tag{2}$$

where G is defined for $z = (z_I)_{I\in\mathcal{P}_n}$ as

$$G(z) = \prod_{I\in\mathcal{P}_n} (1+z_I) z_I^{-b_I-1} \cdot \prod_{J\in\Theta_n^m} \frac{1}{1-\prod_{\substack{I\in\mathcal{P}^n \\ J\subset I}} z_I}.$$

In a second stage, we have proposed an alternative representation formula for the number of m-resilient n-variable Boolean function. More precisely, we have showed that this number can also be interpreted as a coefficient of a term of a multivariate polynomial with integer coefficients:

Proposition 0.3.6.

$$\#Res_n^m = \frac{1}{(2i\pi)^{\#\Gamma_n^m}} \oint P(z) \prod_{I\in\Gamma_n^m} z_I^{-(b_I+1)} \frac{dz}{z}$$

where P is the multivariate polynomial defined as

$$\forall z \in \mathbb{C}, \quad P(z) = \prod_{I\in\Gamma_n^m} (1+z_I) \prod_{J\in\Theta_n^m} \left(1 + \prod_{\substack{I\in\Gamma_n^m \\ J\subset I}} z_I^{a_{I,J}}\right)$$

with

$$\forall (I,J) \in \Gamma_n^m \times \Theta_n^m, \quad a_{I,J} = \binom{\#I - \#J - 1}{n-m-\#J-1}.$$

To conclude, the class of m-resilient Boolean function has been widely studied by cryptographers. Nevertheless, the problem of counting the number of m-resilient n-variable Boolean functions is still challenging. We provide an approach to this question. We reword this question in a problem to count integer solutions of a system of linear inequalities. This allows us to deduce two representation formulas for the number of m-resilient n-variable Boolean functions by means of Cauchy integral. The main difficulty is the large number of variables making it difficult to use directly the known results on this type of integral. New ideas to continue this work are needed.

3- Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity:
The recent algebraic attacks have received a lot of attention in cryptographic literature. The *algebraic immunity* of a Boolean function quantifies its resistance to the standard algebraic attacks of the pseudo-random generators using it as a nonlinear filtering or combining function.

Carlet introduced in [30] the term of *nonlinearity profile* of Boolean functions, which is the sequence whose rth-order term equals the rth-order nonlinearity of the function denote by $nl_r(f)$, and that is the minimum distance between f and all n-variable Boolean functions of algebraic degrees at most r. This parameter extends the standard (first-order) nonlinearity $nl(f)$ of a Boolean function f. Several papers [72, 113, 137, 152, 204] have shown the role played by this parameter in relation to some cryptanalyses (note that contrary to the (first-order) nonlinearity, it must have low value for allowing the attacks to be realistic). Computing theoretically and algorithmically the rth-order nonlinearity of an n-variable Boolean function is a hard task for $r > 1$. Therefore the knowledge of upper and lower bounds for the rth-order nonlinearity on a

particular class of Boolean functions is important.

Very few results have been found concerning its relation with the other cryptographic parameters or with the r-th order nonlinearity. Many recent papers have illustrated the importance of the rth-order nonlinearity profile (which includes the first-order nonlinearity). In 2006, two lower bounds involving the algebraic immunity on the rth-order nonlinearity have been shown by Carlet [30] and Carlet et *al.* [34]. None of them improves upon the other one in all situations.

In 2008, we have proved a new lower bound on the rth-order nonlinearity profile of Boolean functions, given their algebraic immunity, that improves significantly upon one of the known lower bounds for all orders and upon the other one for low orders:

Theorem 0.3.7. *Let f be an n-variable Boolean function of algebraic immunity k and let r be a positive integer strictly less than k. Then*

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$$

To obtain our lower bound, our idea was first to study the dimension $d_{k,g}$ of the annihilators of degrees at most k (denoted by $An_k(g)$) with prescribed algebraic degrees of Boolean functions with given algebraic degrees. In fact, $d_{k,g}$ is an important parameter for evaluating the complexity of algebraic attacks on the systems using a given Boolean function. Moreover, such parameter corresponds to the number of linearly independent low degree annihilators of this Boolean function g and $g \oplus 1$. Little is known on the behavior of $d_{k,g}$. We have proved a simple relation between $d_{k,g}$ and the dimension (denoted by $\dim Mul_k(g)$) of the vector space of all n-variable Boolean functions p that can be written as $p = gh$ where h is of algebraic degree at most k:

Lemma 0.3.8. *3.6.5 Let g be an n-variable Boolean function of algebraic degree r. Let k be any positive integer less than n. Then* $\dim Mul_k(g) = \sum_{i=0}^{k} \binom{n}{i} - d_{k,g}$.

This lead us to derive a lower bound on $d_{k,g}$:

Proposition 0.3.9. *3.6.6 Let g be an n-variable Boolean function of algebraic degree at most r. Then, for every positive integer k, one has $d_{k,g} \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$. If g is the complement of the indicator of an $(n-r)$-dimensional affine subspace of $\mathbb{F}_2^n$ then $d_{k,g} = \sum_{i=0}^{k-r} \binom{n-r}{i}$.*

Next, we have proved a lower bound on the difference $\dim Mul_k(g) - d_{k,1\oplus g}$ valid for every Boolean function of degree at most r.

Corollary 0.3.10. *3.6.9 Let k be a positive integer. Then, for every n-variable Boolean function g of algebraic degree at most r, we have*

$$\dim Mul_k(g) - d_{k,1\oplus g} \geq \sum_{i=k-r+1}^{k} \binom{n-r}{i}$$

At this stage, our approach was to establish a lower bound on $\mathrm{dist}(f, g)$ holding for every Boolean function g of algebraic degree r. To this end, we have established a lower bound on $\mathrm{dist}(f, g)$ involving the sum of the two dimensions $d_{k-1,g}$ and $d_{k-1,1\oplus g}$. This is the key result that enabled us to improve further the lower bounds of Carlet [30] and Carlet et al. [34].

Lemma 0.3.11. *Let f be an n-variable Boolean function. Suppose that $AI(f) = k$. Let r be a positive integer strictly less than k. Then, for every n-variable Boolean function g of algebraic degree at most r, we have*

$$\mathrm{dist}(f, g) \geq d_{k-1,g} + d_{k-1,1\oplus g}.$$

To obtain this result, we have proved the following identity which links $d_{k,f}$ to $rank\,(\Re_f(k,n))$ (where $(\Re_f(k,n))$ denotes the restriction to the support of f of the generator matrix of the kth-order Reed-Muller code of length 2^n, whose the columns correspond to the evaluation of the monomials of algebraic degrees at most k on the support of f).

Proposition 0.3.12. *An n-variable Boolean function f has no annihilator of algebraic degree at most k if and only if all the matrices $\Re_f(r,n)$, $r \leq k-1$, are of full rank. Moreover, one has, for every positive integer $k \leq n$,*

$$d_{k,f} + rank\,(\Re_f(k,n)) \;=\; \sum_{i=0}^{k} \binom{n}{i}. \tag{3}$$

Getting a lower bound on the sum $d_{k-1,g} + d_{k-1,1\oplus g}$ (rather than considering separately the two dimensions $d_{k-1,g}$ and $d_{k-1,1\oplus g}$) enable us to get our new lower bound on $nl_r(f)$.

To conclude, we have studied more deeply than Carlet ([30]) the structure of vector spaces of annihilators with prescribed algebraic degrees for all Boolean functions. Notably, we have established lower and upper bounds on their dimensions (which plays an important role in relation to the rth-order nonlinearity). That allowed us in 2008 to get a new lower bound on the rth-order nonlinearity profile of Boolean functions, given their algebraic immunity, that improves significantly upon one of the known lower bounds for all orders and upon another one for low orders (that is the most interesting case in cryptography). Our results give further information on the relation between the distance of a function to all low-degree functions and its algebraic immunity. It states in particular that it should thus be possible to find Boolean functions having a high algebraic immunity of high nonlinearity and rth-order nonlinearity for low values of r.

4- On a conjecture about binary strings distribution

Building a Boolean function meeting as many criteria as possible is a difficult task. Trade-offs must usually be made between them. Since the introduction of algebraic immunity, several constructions of Boolean functions with high algebraic immunity have been suggested, but very few of them are of optimal algebraic immunity. More importantly, those having other good cryptographic properties, as balancedness or high nonlinearity for instance, are even rarer. Among those having optimal algebraic immunity $AI(f) = \lceil n/2 \rceil$, most have a poor nonlinearity [49, 78, 164, 165, 51], close to the lower bound of Lobanov [172] that is, $\mathrm{nl}(f) \geq 2^{n-1} - \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

We survey in Chapter 3 different known *good* families, i.e. meeting most of the criteria mentioned in a satisfactory way.

In 2010, Tu and Deng [249] discovered that there may be Boolean functions of optimal algebraic immunity in a classical class of Partial Spread functions due to Dillon [86] provided that the following combinatorial conjecture is correct.

Conjecture 0.3.13 (Tu–Deng conjecture)**.** *For all $k \geq 2$ and all $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \,|\, a+b = t \text{ and } \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

Tu and Deng checked the validity of the conjecture for $k \leq 29$. They also proved that, if the conjecture is true, then one can get in even dimension balanced Boolean functions of optimal

algebraic immunity and of high nonlinearity (better than that of the functions proposed by Carlet and Feng [50].

Next, Tang et al. [246] applied a degree optimized version of an iterative construction of balanced Boolean functions with very high nonlinearity by Dobbertin [94] to the functions constructed by Tu and Deng [249, 248] and obtained functions with better nonlinearity.

Unfortunately, Carlet [47] observed that the functions introduced by Tu and Deng are weak against fast algebraic attacks and unsuccessfully tried to repair their weakness. It was subsequently shown by Wang and Johansson [259] that this family can not be easily repaired.

Nonetheless, more recent developments have shown that the construction of Tu and Deng and the associated conjecture are not of purely æsthetic interest, but are interesting tools in a cryptographic context.

In 2011, inspired by the previous work of Tu and Deng [249], Tang, Carlet and Tang [245] constructed an infinite family of Boolean functions with many good cryptographic properties. The main idea of their construction is to change the division in the construction of Tu and Deng by a multiplication. The associated combinatorial conjecture is then modified as follows.

Conjecture 0.3.14 (Tang–Carlet–Tang conjecture)**.** *For all $k \geq 2$ and all $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid a-b=t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

They verified it experimentally for $k \leq 29$, as well as the following generalized property for $k \leq 15$ where $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ is such that $\gcd(u, 2^k-1)=1$ and $\epsilon = \pm 1$.

This generalized conjecture includes the original conjecture proposed by Tu and Deng (Conjecture 3.7.2) for $u=1$ and $\epsilon = +1$.

Finally, Jin et al. [139] generalized the construction of Tang, Carlet and Tang [245] in a way that included back the construction of Tu and Deng [249]. In their paper, the main idea is to replace y by y^{2^k-1-u} in the construction of the function. Hence, the family of Tu and Deng [249] is included for $u=1$, and the family of Tang, Carlet and Tang [245] for $u=2^k-2$. The associated combinatorial conjecture is then modified as follows.

Conjecture 0.3.15 (Jin et al. conjecture)**.** *Let $k \geq 2$ be an integer, $t, u, v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ such that $\gcd(u, 2^k-1) = \gcd(v, 2^k-1) = 1$. Then*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua+vb=t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

This generalized conjecture obviously includes all the previous ones.

The good cryptographic properties of the Boolean functions of the Jin et al. family [138] and more precisely the optimality of their algebraic immunity, depend on the validity of an combinatorial conjecture.

In this context, we have studied[3] these combinatoric problems. More precisely, we have studied the properties of the cardinality of the set $S_{t,v,u,k}$ of interest (that is the set of the generalized

[3] J-P. Flori continued this work in the general case and got a lot of interesting results on this topic in [106]. Unfortunately, there is no complete proof of the conjecture up to now.

Tu–Deng conjecture):

$$S_{t,v,u,k} = \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua+vb = t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1 \right\} \ ,$$

where $k \geq 2$, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ and $u, v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^\times$, i.e. u and v are invertible modulo 2^k-1.

With the above notation, the conjecture of Tu and Deng says that $\#S_{t,+1,1,k} \leq 2^{k-1}$; the conjectures of Tang et al. says that $\#S_{t,-1,1,k} \leq 2^{k-1}$ and $\#S_{t,\epsilon,u,k} \leq 2^{k-1}$ and the one of Jin et al. says that $\#S_{t,v,u,k} \leq 2^{k-1}$.

We have defined the main tool we used to study the conjecture of Tu and Deng[4](this tool is also useful to study the other conjectures):

Definition 0.3.16. *For $a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, we set*

$$r(a,t) = \mathrm{w_H}(a) + \mathrm{w_H}(t) - \mathrm{w_H}(a+t) \ ,$$

i.e. $r(a,t)$ is the number of carries occurring while performing the addition. By convention, we set

$$r(0,t) = k \ ,$$

i.e. 0 behaves like the $\underbrace{\texttt{1...1}}_{k}$ binary string. We also remark that $r(-t,t) = k$.

We have therefore reformulated the conjectures in terms of *carries* occurring in an addition modulo 2^k-1 which gives more insight on it than a simple counting argument. Successful applications of our tools include in particular explicit formulas of $\#S_{t,+1,1,k}$ for numbers whose binary expansion is made of one block, a proof that the conjecture of Tu and Deng is asymptotically true, and a proof that a family of numbers (whose binary expansion has high number of 1s and isolated 0s), reaches the bound of the conjecture. We also conjecture that the numbers in that family are the only ones reaching the bound. Moreover, we provide already enough information which allowed Cohen and Flori to prove very recently that the special case of the conjecture required by the family of Tang, Carlet and Tang [245] is true. Our results contributed to better understanding these conjectures of a combinatorial nature. As far we know, the conjectures presented in this section are still open. Only the variation proposed by Tang, Carlet and Tang has been proved very recently by G. Cohen and J-P. Flori [67].

0.3.2 Publications

The results presented in this chapter have been the subject of the following publications:

- S. Mesnager. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. IEEE Transactions on Information Theory-IT, volume n°54 (8), pages 3656-3662, 2008 ([193]).
- S. Mesnager. On the number of resilient Boolean functions, Journal Number Theory and its Applications World Scientific, volume 5, pages 139-153, 2008 ([194]).
- C. Carlet, P. Guillot and S. Mesnager . On immunity profile of Boolean functions. Proceedings of 4-th International conference SEquences and Their Applications, SETA 2006. LNCS, pages 364-375, Springer, Heidelberg, 2006 ([40]).

[4]In fact, we have studied these combinatorial problems in 2010 therefore, our results have focused on the conjecture of Tu and Deng since the other conjectures were formulated only in 2011.

- J-P. Flori, H. Randriambololona, G. Cohen and S. Mesnager. On a conjecture about binary strings distribution. Proceedings of 6-th International conference SEquences and Their Applications, SETA 2010, LNCS 6338, pages 346-358. Springer, Heidelberg, 2010 ([104]).

0.4 Chapter 4

Bent functions were introduced in the 1960's by Oscar Rothaus [227] in a research not published until 1976 and studied firstly by Dillon in his PhD thesis [82] (1974). They are extremal objects in combinatorics and Boolean function theory. Bent functions have been studied for about 40 years; even more, under the name of difference sets in elementary Abelian 2-groups. The motivation for the study of these particular difference sets is mainly cryptographic (but bent functions play also a role in coding theory and sequences; and as difference sets they lead to designs). Symmetric cryptosystems using Boolean functions can be cryptanalyzed when these Boolean functions can be approximated by affine Boolean functions, that is, by functions of the form $\ell(x_1,\ldots,x_n) = a_0 + a_1x_1 + \cdots + a_nx_n = a_0 + a \cdot x$, where $x = (x_1,\ldots,x_n) \in \mathbb{F}_2^n$, $a = (a_1,\ldots,a_n) \in \mathbb{F}_2^n$ and $a_0 \in \mathbb{F}_2$. The set of affine functions can be viewed as the Reed-Muller code of order 1 (see [98]), denoted by $\mathcal{RM}(1,n)$. We say that ℓ approximates a Boolean function f if the Hamming distance $d_H(f,\ell) = \#\{x \in \mathbb{F}_2^n \mid f(x) \neq \ell(x)\}$ between them is small. So, a Boolean function resists attacks by affine approximation if its distance to $\mathcal{RM}(1,n)$ (i.e. its minimum distance to all affine functions) is large. This distance is called the *nonlinearity* of the function. The maximal possible nonlinearity of n-variable Boolean functions, given by the so-called covering radius bound $2^{n-1} - 2^{n/2-1}$ (see for instance in [31] a survey on Boolean functions), can be achieved with equality for n even only.
A Boolean function f on $\mathbb{F}_2^n$ ($n = 2m$ even) is called bent if its nonlinearity equals $2^{n-1} - 2^{m-1}$ (hence its resistance to the attacks based on affine approximation is optimal). Equivalently, as shown in [82, 227], f is bent if and only if its Walsh transform $\widehat{\chi_f}$ defined at every $a \in \mathbb{F}_2^n$ by $\widehat{\chi_f}(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}$, where "$\cdot$" denotes any inner product in $\mathbb{F}_2^n$ (for instance the inner product defined above), takes values $\pm 2^m$ only (this characterization is independent of the choice of the inner product in $\mathbb{F}_2^n$, since any other inner product has the form $\langle x, s\rangle = x \cdot L(s)$, where L is an auto-adjoint linear automorphism, *i*.e. an automorphism whose associated matrix is symmetric). If f is bent, then the *dual function* $\widetilde{f}$ of f, defined on $\mathbb{F}_2^n$ by: $\widehat{\chi_f}(u) = 2^m(-1)^{\widetilde{f}(u)}$ is also bent and its own dual is f itself.
As any Boolean functions, bent functions can be represented in a unique way by their algebraic normal form (ANF). The global degree of their ANF (called their algebraic degree) is not large: it is upper bounded by m. For this reason (since a cryptographic Boolean function should have high algebraic degree, to allow resistance to the Berlekamp-Massey and Rønjom-Helleseth attacks [179, 226]) and also because bent functions are not balanced, that is, do not have an output uniformly distributed over $\mathbb{F}_2$, they are improper for being used as is in cryptosystems. But they can be used to build proper balanced functions, see [90].
Bent functions are often better viewed in their bivariate representation and can also be viewed in their univariate representation. The univariate representation of any Boolean function is defined as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ (which is an n-dimensional vector space over $\mathbb{F}_2$) and we consider then the input to f as an element of $\mathbb{F}_{2^n}$. An inner product in $\mathbb{F}_{2^n}$ is $x \cdot y = \mathrm{Tr}_1^n(xy)$ where $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. There exists a unique univariate polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ over $\mathbb{F}_{2^n}$ such that f is the polynomial function over $\mathbb{F}_{2^n}$ associated to it (this is true for every function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$). Then the algebraic degree of f equals the maximum 2-weight of the exponents with nonzero coefficients, where the 2-weight $w_2(i)$ of an integer i is the number of 1's in its binary expansion. Hence, in the case of a bent function, all

exponents i whose 2-weights are larger than m have null coefficient a_i. Moreover, f being Boolean, its univariate representation can be written in the form $f(x) = \sum_{j\in\Gamma_n} \mathrm{Tr}_1^{o(j)}(a_j x^j)$, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo 2^n-1, $o(j)$ is the size of the cyclotomic coset of 2 modulo 2^n-1 containing j and $a_j \in \mathbb{F}_{2^{o(j)}}$. This expression is unique. It can also be written under a non-unique form $\mathrm{Tr}_1^n(P(x))$ where $P(x)$ is a polynomial over $\mathbb{F}_{2^n}$.
The bivariate representation of Boolean functions is defined as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and we consider then the input to f as an ordered pair (x, y) of elements of $\mathbb{F}_{2^m}$. There exists a unique bivariate polynomial $\sum_{0\le i,j\le 2^m-1} a_{i,j}x^i y^j$ over $\mathbb{F}_{2^m}$ such that f is the bivariate polynomial function over $\mathbb{F}_{2^m}$ associated to it. Then the algebraic degree of f equals $\max_{(i,j)\,|\,a_{i,j}\neq 0}(w_2(i)+w_2(j))$. And f being Boolean, its bivariate representation can be written in the form $f(x,y) = \mathrm{Tr}_1^m(P(x,y))$ where $P(x,y)$ is some polynomial over $\mathbb{F}_{2^m}$.
The automorphism group of the set of bent functions (i.e., the group of permutations π on $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ such that $f\circ\pi$ is bent for every bent function f) is the general affine group, that is, the group of linear automorphisms composed by translations [31]. The corresponding notion of equivalence between functions is called *affine equivalence*. Also, if f is bent and ℓ is affine, then $f+\ell$ is bent. A class of bent functions is called a *complete class* if it is globally invariant under the action of the general affine group and under the addition of affine functions. The corresponding notion of equivalence is called *extended affine equivalence*, in brief, *EA-equivalence*.
Any function f is bent if and only if, for any nonzero vector a, the Boolean function $D_a f(x) = f(x)+f(x+a)$ is balanced (i.e. has Hamming weight 2^{n-1}). For this reason, bent functions are also called *perfect nonlinear functions*. Equivalently, f is bent if and only if the $2^n \times 2^n$ matrix $H = [(-1)^{f(x+y)}]_{x,y\in\mathbb{F}_2^n}$ is a Hadamard matrix (*i*.e. satisfies $H \times H^t = 2^n I$, where I is the identity matrix), and if and only if the support of f is a *difference set*. Bent functions have also the property that, for every even positive integer w, the sum $\sum_{a\in\mathbb{F}_2^n} \widehat{\chi_f}^{\,w}(a)$ is minimum.

Bent functions are all known for $n \le 8$, only (their determination for 8 variables [215] has been achieved only recently) as well as their classification under the action of the general affine group. For $n \ge 10$, only classes of bent functions are known, which do not cover a large part of them, apparently. Determining all bent functions (or more practically, classifying them under the action of the general affine group) seems elusive. Several constructions of explicit bent functions are known which lead to infinite classes. We describe the main ones in the next section. The two most well-known are the Maiorana-McFarland class and the $\mathcal{PS}_{ap}$ class. Both were studied in Dillon's thesis [82] and have been later revisited in numerous papers.

0.4.1 Summary of the main contributions

1- On Dillon's class H of bent functions, class $\mathcal{H}$ and Niho bent functions
One of the classes of bent Boolean functions introduced by John Dillon in his thesis is family H. While this class corresponds to a nice original construction of bent functions in bivariate form, Dillon could exhibit in it only functions which already belonged to the well-known Maiorana-McFarland class. In fact, the class H is a third family of bent functions introduced by Dillon whose expression is given but whose bentness is achieved under some non-obvious condition (so the class is less explicit than class $\mathcal{M}$ or class $\mathcal{PS}_{ap}$, but it happens to be more explicit than class $\mathcal{PS}$, the condition for H being easier to satisfy than for $\mathcal{PS}$, as we shall see). He defines these functions in bivariate form (but we have observed they can also be seen in univariate form). The functions of this family are defined as $f(x,y) = \mathrm{Tr}_1^m(y + xG(yx^{2^m-2}))$, with $x, y \in \mathbb{F}_{2^m}$ where G is a permutation of $\mathbb{F}_{2^m}$ such that $G(x)+x$ does not vanish and, for every $\beta \in \mathbb{F}_{2^m}^\star$, the function $G(x)+\beta x$ is two-to-one (i.e. the pre-image by this function of any element of $\mathbb{F}_{2^m}$ is either a pair or the empty set).

We have first noticed that H can be extended to a slightly larger class that we denote by $\mathcal{H}$. The definition that we give of the functions in class $\mathcal{H}$ are also in terms of their bivariate representation. More precisely, we call $\mathcal{H}$ the extended class of H equal to the set of functions g defined by (4)

$$g(x,y) = \begin{cases} \mathrm{Tr}_1^m\left(x\psi\left(\frac{y}{x}\right)\right) & \text{if } x \neq 0 \\ \mathrm{Tr}_1^m(\mu y) & \text{if } x = 0 \end{cases} \tag{4}$$

where $\mu \in \mathbb{F}_{2^m}$ and ψ is a mapping from $\mathbb{F}_{2^m}$ to itself satisfying (5) and (6) :

$$G \text{ is a permutation on } \mathbb{F}_{2^m} \text{ where } G \text{ is defined by } G(z) = \psi(z) + \mu z \tag{5}$$

$$\text{For every } \beta \in \mathbb{F}_{2^m}^\star, \text{ the function } z \mapsto G(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m}. \tag{6}$$

Next, we have studied the stability of functions G satisfying Conditions (5) and (6). We have noticed that the transformation which corresponds to applying the same field automorphism to x and y, those which correspond to multiplying x and/or y by constants in $g(x,y)$ and to adding linear functions to g; and the one which corresponds when $G(0) = 0$ to swaping x and y in $g(x,y)$ result in particular cases of EA-equivalence. On the contrary, the bent functions related by transformation $z \mapsto G^{-1}(z)$ are not EA-equivalent, in general. We shall say that two functions G are *o-equivalent* (the reason why we choose such term will come below in sebsection 3) if one can be obtained from the other by a sequence of the transformations $G \mapsto G'$ above. This gives a notion of equivalence of functions in class $\mathcal{H}$ which is not a sub-equivalence of the EA-equivalence of bent functions and is not a super-equivalence either.

Moreover, we have observed that the bent functions constructed via Niho power functions, for which four examples are known due to Dobbertin et al. [93] and to Leander-Kholosha, are the univariate form of the functions of class $\mathcal{H}$. Their restrictions to the vector spaces $\omega\mathbb{F}_{2^{n/2}}$, $\omega \in \mathbb{F}_{2^n}^\star$, are linear.

Since class $\mathcal{H}$ is the set of bent functions whose restrictions to the $\omega\mathbb{F}_{2^m}$'s are linear, a natural extension to consider is the set of those bent functions whose restrictions to the $\omega\mathbb{F}_{2^m}^\star$'s are affine. We have then characterized all the bent functions whose restrictions to the $\omega\mathbb{F}_{2^m}^\star$'s are affine.

2- On the dual of bent functions via Niho exponents

In [93], Dobbertin et al. introduced three classes of binomial Niho[5] bent functions whose expressions (in polynomial forms) are of the type

$$f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)d+1})$$

with $d \in \{\frac{1}{4}, 3, \frac{1}{6}\}$ (where the fractions $\frac{1}{4}$ and $\frac{1}{6}$ are interpreted modulo 2^m+1). The problem of knowing whether the duals of these functions are affinely equivalent to these Niho bent functions was left open since 2006. In a joint work with Carlet, we have answered the open question raised by Dobbertin et al. on whether the duals of the Niho bent functions introduced in the paper are affinely equivalent to them, by explicitely calculating the dual of one of these functions:

Theorem 0.4.1. *Let $n = 2m$ with m odd and f be defined as*

$$\forall t \in \mathbb{F}_{2^n}, \quad f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)\frac{1}{4}+1})$$

[5]The name of Niho exponent comes from a theorem dealing with power functions by Niho [220], which has been later extended to linear combinations of such power functions in [93] (see also [160]), and which relates the value of the Walsh transform of such sum to the number of solutions in U of some equation.

where $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{2^n}^\star$ are such that $b^{2^m+1} = a$ and $b^4 \neq a^2$. Let v be such that $\mathrm{Tr}_m^n(v) = 1$ and $b^4 = a^2 v^{2^m-1}$. Then the dual of f is such that

$$\widetilde{f}(a^{\frac{1}{2}}w) = \mathrm{Tr}_1^m\left(\left(v^{\frac{2^m+1}{2}} + 1 + \mathrm{Tr}_m^n(v^{2^m}w)\right)\left(\frac{\mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}}{\mathrm{Tr}_m^n(v^{-1})}\right)^{\frac{1}{3}}\right).$$

It has algebraic degree $\frac{m+3}{2}$. Hence, for $m > 3$, $\widetilde{f}$ is EA-inequivalent to the functions introduced in [93].

In a joint work with Carlet, Helleseth and Kholosha, we have also computed the dual function of the Niho bent function proposed by Leander and Kholosha in [160] consisting of 2^r exponents and which extends one of the three binomial Niho bent function in [93] (which is obtained with $d = \frac{1}{4}$). The algebraic degree of the dual is calculated and have showed that this new bent function is not of the Niho type.

Theorem 0.4.2. *Let $n = 2m$, $r > 1$ be a positive integer with $\gcd(r, m) = 1$ and bent Boolean function f over $\mathbb{F}_{2^n}$ be defined as*

$$f(t) = \mathrm{Tr}_1^n\left(at^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} t^{(2^m-1)\frac{i}{2^r}+1}\right),$$

where $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. Take any $u \in \mathbb{F}_{2^n}$ with $u + u^{2^m} = 1$. Then the dual of $f(t)$ is equal to

$$\tilde{f}(w) = \mathrm{Tr}_1^m\left(\left(u(1 + w + w^{2^m}) + u^{2^{n-r}} + w^{2^m}\right)(1 + w + w^{2^m})^{1/(2^r-1)}\right).$$

Moreover, if $d < m$ is a positive integer defined uniquely by $dr \equiv 1 \pmod m$ then the algebraic degree of $\tilde{f}(w)$ is equal to $d + 1$.

Finally in a joint work with Carlet and next with Carlet, Helleseth and Kholosha, we have proved that the infinite classes of binomial cubique of Niho bent functions given in [93] and the multinomial Niho bent given [160] belong to the completed Maiorana-McFarland class.

3- Class $\mathcal{H}$ and o-polynomials

Firstly, with Carlet, we have observed that Condition (6) implies Condition (5) and is equivalent to the fact that G is an o-polynomial (also called oval polynomial) which is a notion related to a geometric object from finite projective geometry called *hyperoval*..

Definition 0.4.3. *Let m be any positive integer. A permutation polynomial G over $\mathbb{F}_{2^m}$ is called an o-polynomial (an oval polynomial) if, for every $\gamma \in \mathbb{F}_{2^m}$, the function*

$$z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$$

is a permutation of $\mathbb{F}_{2^m}$.

We then showed that the condition for a function in bivariate form to belong to class $\mathcal{H}$ is equivalent to the fact that a polynomial directly related to its definition is an o-polynomial .

Lemma 0.4.4. *Any function G from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ satisfies Condition* (6) *if and only if it is an o-polynomial.*

We have therefore established a link between a class of bent functions and the notion of o-polynomial from the field of finite geometry.

Thanks to the existence in the literature of 8 classes of nonlinear o-polynomials obtained by the geometers in 40 years, we have deduced a large number of new cases of bent functions in $\mathcal{H}$, which are potentially affinely inequivalent to known bent functions (in particular, to Maiorana-McFarland's functions):

1. $G(z) = z^6$ where m is odd [219];
2. $G(z) = z^{3\cdot 2^k+4}$, where $m = 2k-1$ [111];
3. $G(z) = z^{2^k+2^{2k}}$, where $m = 4k-1$ [111];
4. $G(z) = z^{2^{2k+1}+2^{3k+1}}$, where $m = 4k+1$ [111];
5. $G(z) = z^{2^k} + z^{2^k+2} + z^{3\cdot 2^k+4}$, where $m = 2k-1$ [133];
6. $G(z) = z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}}$ where m is odd [221]; note that $G(z) = D_5\left(z^{\frac{1}{6}}\right)$, where D_5 is the Dickson polynomial of index 5 [224];
7. $G(z) = \frac{\delta^2(z^4+z)+\delta^2(1+\delta+\delta^2)(z^3+z^2)}{z^4+\delta^2z^2+1} + z^{1/2}$, where $\mathrm{Tr}_1^m(1/\delta) = 1$ and, if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$ [262];
8. $G(z) = \frac{1}{\mathrm{Tr}_m^n(v)}\left[\mathrm{Tr}_m^n(v^r)(z+1) + \mathrm{Tr}_m^n\left[(vz+v^{2^m})^r\right]\left(z+\mathrm{Tr}_m^n(v)z^{1/2}+1\right)^{1-r}\right] + z^{1/2}$, where m is even, $r = \pm\frac{2^m-1}{3}$, $v \in \mathbb{F}_{2^{2m}}$, $v^{2^m+1} = 1$ and $v \neq 1$ [263].

For each of the six first o-polynomials G of the list above, we have two potentially new n-variable bent functions: $\mathrm{Tr}_1^m\left(xG\left(\frac{y}{x}\right)\right)$ and $\mathrm{Tr}_1^m\left(xG^{-1}\left(\frac{y}{x}\right)\right)$. For each of the two last ones, we have one potentially new bent function. We indicate now the bent functions we can obtain with the 6 first o-polynomials (we do not do the same for the two last o-polynomials since we conjecture that in these two cases, either G or G^{-1} corresponds to one of the classes of Niho-bent functions from [93] and since the expression of these bent functions would be complex - they are probably simpler in univariate form):

1. for m odd and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{-5}y^6)$;
   - $f(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$.

   The two functions have algebraic degree m, which does not allow proving these two functions are EA-inequivalent; we leave open this question.
2. for $m = 2k-1$ and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$;
   - $f(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$.

   The first function has degree $m-1$ (if $k > 2$) and the second has degree m (if $k > 2$); hence the two functions are EA-inequivalent.
3. for $m = 4k-1$ and $x, y \in \mathbb{F}_{2^m}$:

- $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$;
- $f(x,y) = \mathrm{Tr}_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$.

The two functions are of degree $3k$ which does not allow proving these two functions are EA-inequivalent; we leave open this question.

4. for $m = 4k+1$ and $x, y \in \mathbb{F}_{2^m}$:

   - $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^{2k+1}-2^{3k+1}}y^{2^{2k+1}+2^{3k+1}})$;
   - $f(x,y) = \mathrm{Tr}_1^m(x^{2^{3k+1}-2^{2k+1}+2^k}y^{1-2^{3k+1}+2^{2k+1}-2^k})$.

   The first function has degree $2k+1$ and the second has degree $3k+2$; hence the two functions are EA-inequivalent.

5. for $m = 2k-1$ and $x, y \in \mathbb{F}_{2^m}$:

   - $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^k}y^{2^k} + x^{-(2^k+1)}y^{2^k+2} + x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$;
   - $f(x,y) = \mathrm{Tr}_1^m\left(y\left(y^{2^k+1}x^{-(2^k+1)} + y^3x^{-3} + yx^{-1}\right)^{2^{k-1}-1}\right)$.

   The two functions are of degree m (if $k > 2$). This does not allow proving these two functions are EA-inequivalent; we leave open this question.

6. for m odd and $x, y \in \mathbb{F}_{2^m}$:

   - $f(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}} + x^{\frac{1}{2}}y^{\frac{1}{2}} + x^{\frac{1}{6}}y^{\frac{5}{6}})$;
   - $f(x,y) = \mathrm{Tr}_1^m\left(x\left[D_{\frac{1}{5}}\left(\frac{y}{x}\right)\right]^6\right)$ where $D_{\frac{1}{5}}$ is the Dickson polynomial of index $\frac{1}{5}$, the inverse of 5 modulo $2^{2m}-1$.

   The first function has degree $\max(m, 2, m) = m$, since we already saw that $w_2\left(\frac{1}{6}\right) = \frac{m+1}{2}$ and $w_2\left(\frac{5}{6}\right) = \frac{m-1}{2}$. We leave open the question of an explicit expression of the second and of the determination of its algebraic degree.

4- Niho bent Functions and Subiaco/ Adelaide hyperovals

In a joint work with Helleseth and Kholosha, we have studied the first binomial Niho bent function discovered by Dobbertin et al. that is, the function defined over $\mathbb{F}_{2^n}$ by

$$f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{3(2^m-1)+1})$$

where $a \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_{2^n}^*$ are such that $b^{2^m+1} = a$ and with the condition that if m is even then b is a 5-th power of an element in $\mathbb{F}_{2^n}$. We have showed that the relation between the above binomial Niho bent functions and the o-polynomials give rise to Subiaco class of hyperovals. This allows to expand the original class of bent functions in the case when $m \equiv 2 \pmod 4$ and prove that even in the case when $m \equiv 2 \pmod 4$, the value of b can be taken arbitrary under the condition $b^{2^m+1} = a$:

Theorem 0.4.5. *Let $n = 2m$, $b^{2^m+1} = a$ and $f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{3(2^m-1)+1})$*

1. *Suppose m is odd. Let $v = 1$ and $u \in \mathbb{F}_4 \setminus \{0, 1\}$ then,*

$$G(z) = a^{\frac{1}{2}} + \mathrm{Tr}_m^n(bu) + a^{\frac{1}{2}} f_s(z)$$

If $b = 1$, then

$$G(z) = \frac{z^2 + z}{(z^2 + z + 1)^2} + z^{1/2}$$

is an o-polynomial (thus $f(t)$ bent)

2. *Suppose $m \equiv 2 \pmod 4$. Let $v = 1$, $u \in \mathbb{F}_{16} \setminus \mathbb{F}_4$ with $u^5 = 1$ and $u + u^{2^m} = w$ where $w^2 + w + 1 = 0$. Then*

$$G(z) = a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + (1 + ws + s^{\frac{1}{2}}) \mathrm{Tr}_m^n(b(u^4 + 1)) f_s(z)$$

is an o-polynomial (thus $f(t)$ bent) also for b not a 5-th power.

It is also proven that one of the earlier discovered sporadic Niho bent functions, up to EA-equivalence, belongs to the known infinite class. Moreover, in 2004, using computer calculations, the following sporadic bent function of Niho type was found by Kholosha for $m = 4$: $f(t) = \mathrm{Tr}_1^m(t^{2^m+1}) + \mathrm{Tr}_1^n\left(t^{5(2^m-1)+1} + t^{7(2^m-1)+1}\right)$. The question open since then is whether this function is a new one or if it is EA-equivalent to one of the known Niho bent functions. We resolve this open question by showing that the above function is EA-equivalent to the first binomial Niho bent function (that is, the function defined over $\mathbb{F}_{2^n}$ by $f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{3(2^m-1)+1})$).

Moreover, in the same paper with Helleseth and Kholosha, we have also studied the relation between the second binomial Niho bent function discovered by Dobbertin et al. that is, the function defined over $\mathbb{F}_{2^n}$ by $f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{\frac{1}{6}(2^m-1)+1})$ and o-polynomials and show that give rise to the Adelaide classes of hyperovals.

To conclude this section with Carlet, we introduced a new class $\mathcal{H}$ of bent functions which is larger than that introduced by Dillon in 1974. The elements of the class $\mathcal{H}$ are in bivariate representation and constitute the set of the bent functions whose restrictions to vector spaces (the elements of a spread) $\{E_a = \{(x, ax), x \in \mathbb{F}_{2^m}\}, a \in \mathbb{F}_{2^m}\}$ and $E_\infty = \{(0, y), y \in \mathbb{F}_{2^m}\}$ are linear. In univariate representation, the elements of the class $\mathcal{H}$ coincides with the set of the Niho bent functions. This correspondence has allowed us to answer (first in a work with Carlet, next with Budaghyan, Carlet, Helleseth and Kholosha) to several open questions concerning the known classes of Niho bent functions. This link offers a new general framwork to study the bent functions of Niho type.

Furthermore, we have established with Carlet a link between the elements of the class $\mathcal{H}$ (and thus the set of the Niho bent functions) and o-polynomials which are polynomials associated to particular geometric objects (in the field of Finite Projective Geometry). This link has enabled us to exploit the works about those polynomials from the last 40 years and consequently to exhibit several new families of bent functions in the class $\mathcal{H}$ and thus in the set of the Niho bent fucntions.

5- Bent vectorial functions

Substitution boxes (S-boxes) are fundamental parts of block ciphers. Being the only source of nonlinearity in these ciphers, they play a central role in their robustness, by providing confusion. Mathematically, S-boxes are vectorial (i.e. multi-output) Boolean functions, that is, functions from the vector space $\mathbb{F}_2^n$ (of all binary vectors of length n) to the vector space $\mathbb{F}_2^r$, for given positive

integers n and r. These functions are called (n, r)-functions and include the (single-output) Boolean functions (which correspond to the case $r = 1$). When they are used as S-boxes in block ciphers, their number r of output bits equals or approximately equals the number n of input bits. They can also be used in stream ciphers, with r significantly smaller than n, in the place of Boolean functions to speed up the ciphers.
An (n, r)-function F being given, the *coordinate functions* of F are the Boolean functions $f_1, \cdots, f_r$ defined by $F(x) = (f_1(x), \cdots, f_r(x))$ at every $x \in \mathbb{F}_2^n$. The *component functions* of F are the linear combinations of its coordinate functions, with non all-zero coefficients.
The *nonlinearity* of an S-Box is the minimum nonlinearity of its component functions (that is, the minimum Hamming distance between them and all affine functions). It was introduced and studied initially by Nyberg [212] and further studied by Chabaud and Vaudenay [53]. It constitutes an important parameter in cryptography since it makes possible to quantify the level of resistance of the S-boxes to the linear attack [181]. Bent functions (also called perfect nonlinear functions) are maximally nonlinear multi-output Boolean functions that is, are those functions whose nonlinearity achieves the *covering radius bound* $2^{n-1} - 2^{n/2-1}$ with equality. Equivalently, their derivatives $D_a F(x) = F(x) + F(x + a)$, $a \neq 0$, have uniformly distributed output. Bent (n, r)-functions exist only for even number n of input bits and for $r \leq n/2$ [211]. This restriction makes bent functions often not directly usable as S-boxes in block ciphers, but these functions have however great cryptographic interest because, contributing to an optimum resistance (among all functions, whatever are the numbers of input and output bits) to the linear and differential attacks of those cryptosystems in which they are involved, they can be used to build (n, n)-functions which have, among (n, n)-functions, optimal resistance to these attacks (see [32]).

The problem of constructing vectorial bent functions has received a lot of attention in the literature. One distinguishes two kinds of constructions of bent functions (or more generally of vectorial functions satisfying some criteria): primary constructions, which do not need to use previously constructed functions for designing new functions, and secondary constructions (of new functions from two or several already known ones, used as building blocks).

To classify vectorial Boolean functions that satisfy desirable nonlinearity conditions, or to determine whether, once found, they are essentially new (that is, inequivalent in some sense to any of the functions already found) we use some concepts of equivalence. For vectorial Boolean functions, the most useful concepts of equivalence are the extended affine EA-equivalence and the CCZ-equivalence. Two (n, r)-functions F and F' are called EA-equivalent if there exist affine automorphisms L from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ and L' from $\mathbb{F}_2^r$ to $\mathbb{F}_2^r$ and an affine function L'' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^r$ such that $F' = L' \circ F \circ L + L''$. EA-equivalence is a particular case of CCZ-equivalence [33]. Two (n, r)-functions F and F' are called CCZ-equivalent if their graphs $G_F := \{(x, F(x)),\ x \in \mathbb{F}_2^n\}$ and $G'_F := \{(x, F'(x)),\ x \in \mathbb{F}_2^n\}$ are affine equivalent, that is, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^r$ such that $\mathcal{L}(G_F) = G'_F$. The nonlinearity is invariant under CCZ equivalence (and hence under extended affine equivalence). Recently, Budaghyan and Carlet have proved in [12] that for bent vectorial Boolean functions, CCZ-equivalence coincides with EA-equivalence and that they coincide for Boolean function (any of them) as well [13].

The known primary constructions of bent vectorial functions come essentially from known constructions of Boolean functions extended to the context of vectorial functions. As observed firstly by Nyberg in [211], the two main classes of bent Boolean functions lead to two classes of bent vectorial functions. The first one comes from the well known *Maiorana-McFarland* class of bent Boolean functions and gives bent vectorial functions belonging to the class that we shall call the *strict Maiorana-McFarland* of vectorial bent functions. Such construction can be generalized to functions belonging to the *general Maiorana-McFarland* class of vectorial bent functions. In fact, a third class can be identified, nested between these two classes (we shall call it the *extended*

Maiorana-McFarland class). The second well-known class comes from the so-called *Dillon Partial Spread class* $\mathcal{PS}_{ap}$ of bent Boolean functions. Its extension to the context of vectorial functions gives bent functions whose component functions belong to this class.

We have studied more in details and generalized the known primary constructions of vectorial bent functions. In particular, we have proposed another Partial Spread construction of bent vectorial functions as well as other primary constructions of bent functions. Concerning the secondary constructions of bent (n, r)-functions, the known ones are also mostly derived as generalizations of the known secondary constructions of bent Boolean functions. Finding new secondary constructions of bent vectorial functions is not a simple task. We have studied more in details and generalized the known secondary constructions of bent vectorial functions, and we have introduced new ones.

Very recently, we have proved that o-polynomials lead to primary constructions of optimal bent vectorial functions that is, bent functions vectorial from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$.

Theorem 0.4.6. *Let G be an o-polynomial. Let F, F' be two vectorial functions from $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ such that for $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,*

$$F(x, y) = xG(yx^{2^m-2})$$

and

$$F'(x, y) = xG^{-1}(yx^{2^m-2})$$

Then, the (n, m)- functions F and F' are bent.

0.4.2 Publications

The results presented in Chapter 4 have been the subject of the following publications:

- C. Carlet and S. Mesnager. On Dillon's class H of bent functions, Niho bent functions and o-polynomials. Journal of Combinatorial Theory-JCT-serie A 118, pages 2392–2410, 2011([44]).

- C. Carlet and S. Mesnager. On the construction of bent vectorial functions. Journal of Information and Coding Theory: Algebraic and Combinatorial Coding Theory, volume 1, No. 2, pages 133-148, 2010 ([16]).

- T. Helleseth, A. Kholosha and S. Mesnager. Niho Bent Functions and Subiaco/Adelaide Hyperovals. Proceedings of the 10-th International Conference on Finite Fields and Their Applications (Fq'10) Contemporary Math., AMS, 2012. Vol 579, pages 91-101, 2012. ([126]).

- C. Carlet, T. Helleseth, A. Kholosha and S. Mesnager. On the Dual of Bent Functions with 2^r Niho Exponents. IEEE International Symposium on Information Theory, ISIT 2011, pages 703-707, Saint-Petersturg, Russie, 2011([41]).

- L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha and S. Mesnager. Further results on Niho bent functions. IEEE Transactions on Information Theory-IT. Vol. 58 no. 11, pages 6979–6985, 2012 ([14]).

0.5 Chapter 5

Hyper-bent functions were introduced by Youssef and Gong [271] at Eurocrypt' 01 in 2001 but the first definition of hyperbent functions was based on a property of the so-called extended Hadamard transform of f which was introduced in [115] by Golomb and Gong. Hyper-bent functions are both of theoretical and practical interest. They were initially proposed by Golomb and Gong as a component of S-boxes to ensure the security of symmetric cryptosystems. Such functions are interesting from a combinatorial point of view: they indeed have stronger properties than the well-known bent functions which were already studied by Dillon and Rothaus more than three decades ago. Hyper-bent functions are indeed bent up to to a change a primitive root in $\mathbb{F}_{2^n}$. The idea behind the hyper-bent functions is to maximize the minimum distance to all Boolean functions coming from bijective monomials on $\mathbb{F}_{2^n}$ (that is, bijective functions whose expression is the absolute trace of a single power function), not just the affine functions (that is, functions of the form $\mathrm{Tr}_1^n(ax)+\epsilon$; $a \in \mathbb{F}_{2^n}$, $\epsilon \in \mathbb{F}_2$). Bent are rare but hyper-bent functions are still rarer. These functions are not classified. A complete classification of these functions is elusive and looks hopeless. So, it is important to design constructions in order to know as many (hyper)-bent functions as possible. And not only their characterization, but also their generation are challenging problems.

0.5.1 Summary of the main contributions

Our first contribution is the construction of hyper-bent functions over $\mathbb{F}_{2^n}$ $(n = 2m)$ having the form $f(x) = \mathrm{Tr}_1^{o(s_1)}(ax^{s_1}) + \mathrm{Tr}_1^{o(s_2)}(bx^{s_2})$ where $o(s_i)$ denotes the cardinality of the cyclotomic class of 2 modulo $2^n - 1$ which contains s_i and whose coefficients a and b are, respectively in $F_{2^{o(s_1)}}$ and $F_{2^{o(s_2)}}$. Few constructions of hyper-bent functions defined over the Galois field $\mathbb{F}_{2^n}$ $(n = 2m)$ are proposed in the literature. The known ones are mostly monomial functions.

As mentioned by Charpin and Gong in [54], it seems difficult to define an infinite class of hyper-bent functions. In fact, since 2001 [271], very few infinite classes of hyper-bent Boolean functions have been presented in the literature. The known hyper-bent Boolean functions are mostly monomial functions of Dillon (that is of the form $\mathrm{Tr}_1^n(ax^{2^m-1})$ generalized further by Charpin and Gong into $\mathrm{Tr}_1^n(ax^{r(2^m-1)})$ (with r co-prime with 2^m+1). Dillon monomial (hyper-)bent functions belong all to the $\mathcal{PS}_{ap}$ class and they are related to the zeros of some Kloosterman sums (see [82],[54],[159]). In 2008, Charpin and Gong [55, 54] have provided new interesting tools to describe hyper-bent Boolean functions with multiple trace terms (which are the sum of several Dillon monomial functions) by means of Dickson polynomials. They have studied precisely Boolean functions defined on $\mathbb{F}_{2^n}$ whose expression is of the form $\sum_{r\in E} \mathrm{Tr}_1^n(\beta_r x^{r(2^m-1)})$, where E is a subset of the set of representatives of the cyclotomic cosets modulo 2^m+1 of maximal size $n = 2m$, and the coefficients β_r are in $\mathbb{F}_{2^n}$. As a consequence of their new interesting approach, a characterization of a class of binomial hyper-bent functions has been obtained. But the precise characterization of such multinomial functions which are hyper-bent, by giving explicitly the coefficients β_r, is still an open problem (see [54]).

In 2009, we have proved firstly that the exponents $s_1 = 2^{\frac{n}{2}} - 1$ and $s_2 = \frac{2^n-1}{3}$, where $a \in \mathbb{F}_{2^n}$ $(a \neq 0)$ and $b \in \mathbb{F}_4$, provide a construction of a first family (denoted by $\mathfrak{F}_n$) of binomial hyper-bent functions over $\mathbb{F}_{2^n}$ (with optimum algebraic degree) defined by

$$f_{a,b}(x) = \mathrm{Tr}_1^n(ax^{2^m-1}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$$

In the line of the results of Dillon [82] on monomials bent functions via Dillon exponents, we

have showed that the bentness of a Boolean function $f_{a,b}$ of the family $\mathfrak{F}_n$ can be characterized by means of the *Kloosterman sums* involving only the coefficient a when m is odd. To this end, we have showed first that $\mathfrak{F}_n$ is a subclass of the well known Partial Spreads class for which the bentness of its functions can be characterized by means of the Hamming weight of their restrictions to a certain set. Next, we have investigated the conditions on the choice of a and b for obtaining an explicit family of bent functions. Thanks to the recent works of Charpin, Helleseth and Zinoviev on the Kloosterman sums and cubic sums, we have established an explicit characterization of the bentness of functions belonging to $\mathfrak{F}_n$ in terms of the Kloosterman sums of the coefficient a when m is odd. Next, we have generalized the results for functions whose exponent s_1 is of the form $r(2^m-1)$ where r is co-prime with 2^m+1. The corresponding bent functions are also hyper-bent.

The following theorem summarizes the results of our study related to the bentness of the functions of the family $\mathfrak{F}_n$.

Theorem 0.5.1. *Let $n=2m$ with m odd ($m>3$). Let $a\in\mathbb{F}_{2^m}^\star$ and $b\in\mathbb{F}_4^\star$. Let $f_{a,b}^{(r)}$ be the function defined on $\mathbb{F}_{2^n}$ by (5.10) $f_{a,b}^{(r)}(x)=\mathrm{Tr}_1^n(ax^{r(2^m-1)})+\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$*

1. *$f_{a,b}^{(r)}$ is bent if and only if $K_m(a)=4$.*
2. *$f_{a,b}^{(r)}$ is hyper-bent if and only if $f_{a,b}^{(r)}$ is bent.*
3. *The bent functions $f_{a,b}^{(r)}$ are in the class $\mathcal{PS}^-$. Moreover, the bent functions $f_{a,b}^{(r)}$ are elements of the Partial Spread class $\mathcal{PS}_{ap}$ (resp. $\mathcal{PS}_{ap}^{\#}$) if $b=1$ (resp. if $b\neq 1$).*
4. *If $f_{a,b}^{(r)}$ is bent then its dual function equals $f_{a^{2^m},b^2}^{(r)}$.*

When m is even, we have shown that the situation seems to be more complicated theoretically than in the case where m is odd, and that the study of the bentness cannot be done as in the odd case. However, in this case, we are nevertheless able to show that a Boolean function whose expression is of the form $\mathrm{Tr}_1^n(ax^{2^m-1})+\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$, cannot be bent if the condition of bentness in terms of Kloosterman sums that we got in the odd case is not satisfied. More precisely, we have showed that the value 4 is still a necessary condition for bentness. In the continuation of this work, we have studied more deeply theoretically the bentenss of functions in $\mathfrak{F}_n$ in the case when m is even and provide results from experimental investigations[6]. But it is an open problem to tell whether this condition is sufficient for all m even or not. Therefore we conducted experiments to find all the values 4 of binary Kloosterman sums and test the corresponding Boolean functions for m even as big as possible. All the values we tested gave bent functions, pointing out that the situation in the case m even should definitely be studied further.

Next, in late 2009, we have proved that the exponents $s_1=3(2^m-1)$ and $s_2=\frac{2^n-1}{3}$, where $a\in\mathbb{F}_{2^n}$ ($a\neq 0$) and $b\in\mathbb{F}_4$ provide a construction of another family $\mathfrak{G}_n$ of hyper-bent functions over $\mathbb{F}_{2^n}$ (and all the functions of $\mathfrak{G}_n$ are of optimum algebraic degree). Functions of $\mathfrak{G}_n$ are of the form

$$g_{a,b}(x)=\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

Since m being odd, 3 is a divisor of 2^m+1 so functions of $\mathfrak{F}_n$ and $\mathfrak{G}_n$ are not in the class studied by Charpin and Gong [54] that we have mentioned above. We have studied functions of $\mathfrak{G}_n$ and obtained an explicit characterization of the bentness of these functions, in terms

[6] the implementation was made using Sage [241] and Cython [9], performing direct calls to Givaro [96], NTL [235] and gf2x [10] libraries for efficient manipulation of finite field elements and construction of Boolean functions.

of the Kloosterman sums and the cubic sums involving only the coefficient a. The following theorem recapitulates the results of our study in which we prove that class $\mathfrak{G}_n$ contains hyper-bent functions when $m \not\equiv 3 \pmod 6$ while there is no hyper-bent functions in this class when $m \equiv 3 \pmod 6$; an important point is that this class does not contain other bent functions except those which are hyper-bent.

Theorem 0.5.2. *Let $n = 2m$. Suppose that m is odd. Let $a \in \mathbb{F}_{2^m}^\star$. Let β be a primitive element of $\mathbb{F}_4$. Let ζ be a generator of the cyclic group U of (2^m+1)-th of unity. For $(i,j) \in \{0,1,2\}^2$, let $g_{a\zeta^i,\beta^j}$ be a Boolean function on $\mathbb{F}_{2^n}$ of $\mathfrak{G}_n$*

1. *Assume $m \not\equiv 3 \pmod 6$. Then, we have:*
   - *If $\mathrm{Tr}_1^m(a^{1/3}) = 0$ then, for every $(i,j) \in \{0,1,2\}^2$, a function $g_{a\zeta^i,\beta^j}$ is (hyper)-bent if and only if $K_m(a) = 4$.*
   - *If $\mathrm{Tr}_1^m(a^{1/3}) = 1$ then:*
     (a) g_{a,β^j} is not bent for every $j \in \{0,1,2\}$.
     (b) For every $i \in \{1,2\}$, $g_{a\zeta^i,\beta^j}$ is (hyper)-bent if and only if $K_m(a) + C_m(a,a) = 4$.
2. *Assume $m \equiv 3 \pmod 6$. Then, for every $i \in \{0,1,2\}$, $g_{a\zeta^i,b}$ is not bent for every $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$.*

The dual function of a bent function $g_{a,b}$ of $\mathfrak{G}_n$ is equal $g_{a^{2^m},b^2}$

To conclude, in these works, we contribute to the knowledge of the class of hyper-bent Boolean functions by exhibiting two new infinite family of hyper-bent Boolean functions defined on $\mathbb{F}_{2^n}$ when $m = n/2$ is odd (that does not belong to the class studied in [54]) in which the property to be hyper-bent is strongly related to the Kloosterman sums. In particular, we extend the known link between Dillon monomial hyper-bent functions and the zeros of Kloosterman sums to others values and to other functions. In addition, it is important to point out that, unlike the family of hyper-bent functions of $\mathfrak{F}_n$, the monomial functions of $\mathfrak{G}_n$ are never bent (and then are not hyper-bent) since the exponent does not satisfy the necessary condition for a bent exponent. We have also studied the normality of functions in $\mathfrak{F}_n$ and $\mathfrak{G}_n$ and we have computed their corresponding duals functions.

0.5.2 Publications

The results presented in Chapter 5 have been the subject of the following publications:

- S. Mesnager. A new family of hyper-bent Boolean functions in polynomial form. Proceedings of Twelfth International Conference on Cryptography and Coding. Cirencester, United Kingdom. M. G. Parker (Ed.) IMACC 2009, LNCS 5921, pages 402–417. Springer, Heidelberg (2009) ([196]).
- S. Mesnager. A new class of Bent Boolean functions in polynomial forms. Proceedings of international Workshop on Coding and Cryptography, WCC 2009, pages 5-18, Ullensvang, Norway, pages 5–18, 2009([195]).
- S. Mesnager. A New Class of Bent and Hyper-Bent Boolean Functions in Polynomial Forms. Journal Designs, Codes and Cryptography (DCC) volume 59, Numbers 1-3, pages 265-279, 2011([197]).

0.6 Chapter 6

0.6.1 Summary of the main contributions

As mentioned above, Charpin and Gong [54] have studied the bentness of the class of Boolean functions defined on $\mathbb{F}_{2^n}$ by

$$\sum_{r\in R} \mathrm{Tr}_1^n(\beta_r x^{r(2^m-1)})$$

where $n := 2m$ and R is a subset of a set of representatives of the cyclotomic cosets modulo 2^m+1 for which each coset has the full size $n = 2m$ and $\beta_r \in \mathbb{F}_{2^n}$. When r is co-prime with 2^m+1, the functions f are the sums of several Dillon monomial functions. A new tool by means of Dickson polynomials to describe hyper-bent functions f has been introduced in [54]. In fact, Charpin and Gong have shown that the bentness of those functions is related to the Dickson polynomials under some restriction on the coefficients β_r (more precisely, $\beta_r \in \mathbb{F}_{2^m}$). In the line of our results in the binomial case and of the results of Charpin and Gong, we have studied a subclass $\mathfrak{H}_n$ of the so-called class PS^-. Functions of $\mathfrak{F}_n$ are with multiple trace terms of the form

$$\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$$

where R is a set of representatives of the cyclotomic cosets modulo 2^n-1 of maximal size $n := 2m$, $\{a_r,\, r \in R\}$ is a collection of elements of $\mathbb{F}_{2^m}$ and b is an element of $\mathbb{F}_4$. The set of the functions $\mathfrak{H}_n$ includes the families $\mathfrak{F}_n$ and $\mathfrak{G}_n$. We have studied the hyper-bentness property of functions in $\mathfrak{H}_n$ and showed that hyper-bent functions of $\mathfrak{H}_n$ can be described by means of exponential sums involving Dickson polynomials of degree r and 3. In particular, when b is a primitive element of $\mathbb{F}_4$, we provide a way to transfer the characterization of hyper-bentness of an element of $\mathfrak{G}_n$ to the evaluation of the Hamming weight of some Boolean functions.

The following theorem summarizes our study of the bentness of functions in $\mathfrak{H}_n$

Theorem 0.6.1. *Let $n = 2m$ with m odd. Let $b \in \mathbb{F}_4^\star$ and β be a primitive element of $\mathbb{F}_4$. Let $f_{a_r,b}$ be a function of $\mathfrak{H}_n$ defined on $\mathbb{F}_{2^n}$ by (6.2). Let g_{a_r} be the related function defined on $\mathbb{F}_{2^m}$ by $g_{a_r}(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r.*

1. *$f_{a_r,b}$ is hyper-bent if and only if $f_{a_r,b}$ is bent.*
2. *The bent functions $f_{a_r,b}$ are in the class $\mathcal{PS}^-$. Moreover, the bent functions $f_{a_r,b}$ are elements of the Partial Spread class $\mathcal{PS}_{ap}$ (resp. $\mathcal{PS}_{ap}^{\#}$) if $b = 1$ (resp. if $b \neq 1$).*
3. *The three following assertions are equivalent:*
   (a) *$f_{a_r,\beta}$ is hyper-bent;*
   (b) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g_{a_r}(D_3(x))\Big) = -2;$
   (c) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + g_{a_r}(D_3(x))\Big) = 2^m - 2\,\mathrm{wt}(g_{a_r}\circ D_3) + 4.$
4. *$f_{a_r,1}$ is hyper-bent if and only if,* $2\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g_{a_r}(D_3(x))\Big) - 3\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g_{a_r}(x)\Big) = 2.$

Note that the previous theorem is valid when the coefficients a_r are elements of $\mathbb{F}_{2^m}$.

To illustrate our results, we have showed that our results presented for the families $\mathfrak{F}_n$ and $\mathfrak{G}_n$ can be deduced. In particular, the link between the binomial hyper-bent functions of $\mathfrak{F}_n$ (resp. $\mathfrak{G}_n$) and the value 4 of some Kloosterman sums has been generalized to a link between hyper-bent functions of $\mathfrak{H}_n$ and some exponential sums where Dickson polynomials are involved. Finally, we have provided possibly new infinite families of hyper-bent functions provided that some set is not empty. Our study extends our works in the binomial case and is a complement of the work of Charpin and Gong on this topic.

Adopting our approach presented above on the study of functions in $\mathfrak{H}_n$, Wang,Tang, Qi, Yang and Xu [258] have studied in late 2011 the following family with an additional trace term on $\mathbb{F}_{16}$:

$$f_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) + \mathrm{Tr}_1^4 \left(b x^{\frac{2^n-1}{5}} \right)$$

where the coefficients a_r lie in $\mathbb{F}_{2^m}$, the coefficient b is in $\mathbb{F}_{16}$ and m must verify $m \equiv 2 \pmod 4$. The set R is defined as above (that is, a subset of representatives of the cyclotomic cosets modulo $2^m + 1$ for which each coset has the maximal size n).

In a joint work with Flori, we have provided a finer study of the family of Wang et al. by giving results including useful expressions for their extended Walsh-Hadamard transform, their algebraic degrees and their duals.

Very recently, we have been interested to the generalization of all the hyper-bent functions with multiple trace terms (including binomial functions) via Dillon-like exponents that is, exponents of the generalized form $s(2^m - 1)$. More precisely, we have studied functions of the general form:

$$f_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) + \mathrm{Tr}_1^t \left(b x^{s(2^m-1)} \right)$$

where $n = 2m$ is an even integer, R is a set of representatives of the cyclotomic classes modulo $2^m + 1$, the coefficients a_r are in $\mathbb{F}_{2^m}$, s divides $2^m + 1$, i.e. $s(2^m - 1)$ is a Dillon-like exponent, $t = o(s(2^m - 1))$, i.e. t is the size of the cyclotomic coset of s modulo $2^m + 1$, and the coefficient b is in $\mathbb{F}_{2^t}$.

We have showed how the approach that we have developed in 2009 extend the Charpin-Gong family (2008) and subsequently slightly extended by Wang et al. (2011) using our approach fits in a much more general setting and we have presented generalizations of the previous approaches in different directions.To this end, firstly we have observed that the original restriction for Charpin–Gong criterion can be weakened before generalizing our approach to arbitrary Dillon-like exponents. Afterward, we have tackled the problem of devising infinite families of extension degrees for which a given exponent is valid and apply these results not only to reprove straightforwardly our results and those of Wang et al., but also to characterize the hyper-bentness of several potentially new infinite classes of Boolean functions. We go into full details for a few of them, provide as well an algorithm and the corresponding software to extend this approach to an infinity of other new families.

0.6.2 Publications

The results presented in Chapter 6 have been the subject of the following publications:

- S. Mesnager. Hyper-bent Boolean Functions with Multiple Trace Terms. Proceedings of International Workshop on the Arithmetic of Finite Fields. WAIFI 2010, LNCS 6087, pages. 97–113. Springer, Heidelberg, 2010 ([192]).
- S. Mesnager Bent and Hyper-bent Functions in polynomial form and Their Link With Some Exponential Sums and Dickson Polynomials. IEEE Transactions on Information Theory-IT, Vol 57, No 9, pages 5996-6009, 2011 ([198]).
- S. Mesnager and J.P Flori. On hyper-bent functions via Dillon-like exponents. IEEE International Symopsium on Infomation Theory ISIT 2012. IMT, Cambridge, MA, USA, 2012 ([202])

0.7 Chapter 7

The connection between exponential sums and algebraic varieties has been known for at least six decades. Connecting exponential sums and numbers of points on algebraic varieties is classical folklore. Such ideas go back, at least, to the work of Weil [264] where the Riemann hypothesis is used to bound the values of Kloosterman sums. Leonard and Williams [161] then devised the connection between Kloosterman sums and elliptic curves, and Lachaud and Wolfmann [157], and Katz and Livné [146], exploited the theory of elliptic curves to study the distribution of Kloosterman sums. Very recently, Lisoněk [170] followed this approach to reformulate the Charpin–Gong characterization of a large class of hyper-bent functions in terms of numbers of points on hyperelliptic curves. As a consequence, he obtained a polynomial time and space algorithm for certain subclasses of functions in the Charpin–Gong family.

0.7.1 Summary of the main contributions

In Chapter 7, we settle a more general framework, together with detailed proofs, for such an approach and present a more generic formulation of the connection between Boolean functions, exponential sums and hyperelliptic curves. This leads us to easily deduce the previous results of Lisoněk, as well as giving an efficient version of the more recent hyper-bentness criterion that we have proposed. Doing so, a polynomial time and space test for the hyper-bentness of functions in the family $\mathfrak{H}_n$ is obtained as well. Nonetheless, a straightforward application of such results does not provide a satisfactory criterion for explicit generation of functions in our family $\mathfrak{H}_n$. To address this issue, we have showed how to obtain a more efficient test leading to a substantial practical gain and subsequently propose a slightly different reformulation leading to practical speed-ups. The algorithmic theory of such curves shows that this reformulation gives rise to a test in both polynomial time and space when restricted to certain subclasses of functions.

Next, we have extended reformulations in terms of hyperelliptic curves of the aforementioned hyper-bentness characterizations[7], previously proposed by Lisoněk [170] and Flori and the author to the characterization proposed by Wang et al. A fundamental object in these works are Dickson polynomials. A good understanding of their properties, and in particular of those involving the subsets of finite fields composed of elements whose inverses have a given trace, was therefore crucial. We have used our study about the action of Dickson polynomials on subsets of finite fields of even characteristic related to the trace of the inverse of an element and apply such properties

[7]In chronological order of our results, we have firstly adapted the approach of Linonek in the framework of semi-bent functions

to the study of the Wang et al.'s family and a characterization of their hyper-bentness in terms of exponential sums. Moreover, we have provided numerical evidence that the characterizations using hyperelliptic curves are more efficient than those involving exponential sums not only asymptotically, but also for practical values of m.

Finally (following our works on hyper-bent functions), we have been interested to treat the general case of hyper-bent functions with multiple trace terms via Dillon-like exponents and provided both known and new applications of our developed theory. Moreover, we have showed how to transform the obtained characterizations in terms of hyperelliptic curves, providing both an analysis of the asymptotic complexity of the generation of hyper-bent functions and experimental results for their practical generation.

In all these works, our reformulations of such characterizations in terms of cardinalities of hyperelliptic curves are based on the classical connection between exponential sums and algebraic varieties. We use these connections as well as properties of Dickson polynomials and the trace of inverse to actually build hyper-bent functions in cases which could not be attained through naive computations of exponential sums.

In the last part of Chapter 7, we recall classical results about divisibility of binary Kloosterman sums[8] and give alternate proofs of such results involving the theory of elliptic curves. We analyze the different strategies used to find zeros of binary Kloosterman sums to develop and implement an algorithm to find the value 4 of such sums. We present different algorithms to test and find specific values of binary Kloosterman sums. Then, emphasizing the specificity of the zero case, we study the use of elliptic curves involved in this case, explain which results can be extended to the value 4, develop and implement an algorithm to find that value.

0.7.2 Publications

The results presented in Chapter 7 have been the subject of the following publications:

- J.P. Flori and S. Mesnager. Dickson polynomials, hyperelliptic curves and hyper-bent functions. Proceedings of 7-th International conference SEquences and Their Applications, SETA 2012, LNCS 7280, Springer, pages 40–52, 2012 [102].

- J.P. Flori, S. Mesnager and G. Cohen. Binary Kloosterman sums with value 4. Proceedings of Thirteenth International Conference on Cryptography and Coding, IMACC 2011, LNCS 7089, pages 61-78, Springer, 2011[103].

0.8 Chapter 8

A number of research works in symmetric cryptography are devoted to problems of resistance of various ciphering algorithms to the fast correlation attacks (on stream ciphers) and to the linear cryptanalysis (on block ciphers). These works analyse various classes of approximating functions and constructions of functions with the best resistance to such approximations. Some general classes of Boolean functions play a central role with this respect: the class of *bent functions* [227],

[8]Kloosterman sums have recently become the focus of much research, most notably due to their applications in cryptography and their relations to coding theory. In our very recent works we have showed that the value 4 of binary Kloosterman sums gives rise to several infinite classes of bent functions, hyper-bent functions and semi-bent functions in even dimension.

its subclasses of homogeneous bent functions [223] and hyper-bent functions [271], and the generalizations of the notion: semi-bent functions [62], Z-bent functions [92], negabent functions [218], etc.

In this chapter we investigate constructions of *semi-bent functions* in even dimension. The term of semi-bent function has been introduced by Chee, Lee and Kim at Asiacrypt' 94 [62]. These functions had been previously investigated under the name of 3-valued almost optimal Boolean functions in [19]. Also, they are particular cases of the so-called plateaued functions [276, 275]. They are nice combinatorial objects, as are bent functions. They are studied in cryptography because, besides having low Walsh Hadamard transform which provides protection against fast correlation attacks [188] and linear cryptanalysis [182], they can possess desirable properties (in addition to the propagation criterion of high order and to low additive autocorrelation), such as balancedness, resiliency. They share with bent functions the cryptographic drawback of having algebraic degree at most $n/2$. (as bent functions, they can be used in the constructions of Boolean functions with good cryptographic properties [31]) Several general constructions of semi-bent functions in even dimension exist: partially-bent functions [31] with linear kernels of dimension 2, restrictions of bent functions to vector subspaces $\{a, b\}^{\perp}$ of co-dimension 2 such that the second-order derivative $D_a D_b \widetilde{f}$ of the dual $\widetilde{f}$ of the bent function is null [19, 20]; In [59], Charpin et al gave a necessary and sufficient condition for a class of quadratic functions in even number of variables to be semi-bent; some more specific constructions are also known [62, 242]; but the functions which can be constructed so far are most probably very rare among all semi-bent functions. Semi-bent functions can be defined for n even and for n odd (n being the number of the inputs). By Parseval's relation, the maximum magnitude of the Walsh Hadamard transform of n-variable Boolean functions is at least $2^{\frac{n}{2}}$. This lower bound is achieved with equality only when n is even, by the so-called bent functions. It is well-known that the Walsh Hadamard transform of a bent function only takes on the values $\pm 2^{\frac{n}{2}}$. Bent functions are never balanced. When n is even, the semi-bent functions are those Boolean functions whose Walsh Hadamard transform takes values 0 and $\pm 2^{\frac{n+2}{2}}$. They are balanced (up to the addition of a linear function) and have the maximal non-linearity that balanced plateaued functions can have. When n is odd, the lower bound for the maximum magnitude of the Walsh Hadamard transform is not known in general. However, this lower bound has been shown to be $2^{\frac{n+1}{2}}$ when the function is quadratic [176] or for small values of n [209]. Functions which achieve this lower bound with equality are the semi-bent functions, whose Walsh Hadamard transform only takes on the three values 0, $\pm 2^{\frac{n+1}{2}}$ [63]. Some research has been devoted to finding new families of semi-bent functions and semi-bent sequences. In fact, highly nonlinear functions (that is, functions having large Hamming distances from the set of affine Boolean functions, or in other terms large non-linearity) correspond in the theory of sequences, to sequences that have low cross-correlation with the m-sequences (maximum-length linear feedback shift register sequences) represented by $\mathrm{Tr}_1^m(x)$ [127] [125]. The main contributions in this direction are due to Gold [112], Niho [210], Helleseth [124, 125], Helleseth and Kumar [127]. However, almost all families of semi-bent functions have been derived from power polynomials, that is, $x \mapsto \mathrm{Tr}_1^n\left(x^d\right)$ for a suitably chosen d and when n is odd. Khoo, Gong and Stinson [149] have exhibited a new family of semi-bent Gold-like sequences and have characterized in [150] semi-bent quadratic functions with odd number of inputs; more precisely, $\mathbb{F}_2$-linear combinations of Gold functions. In [59], Charpin, Pasalic and Tavernier have expanded the result of Khoo et al. [149] on quadratic functions in many directions. In particular, they have generalized a result on quadratic semi-bent functions to the case n even, given some new infinite classes of quadratic semi-bent functions for n odd and shown that some infinite classes of quadratic semi-bent functions may be derived by composing a quadratic semi-bent function with certain non-bijective linear polynomials. Moreover, they have shown how to generate a cubic semi-bent function in $n+1$ variables by the concatenation of two suitably chosen quadratic

bent or semi-bent functions in n variables. The treatment of n-variable semi-bent functions was presented in a much wider framework in the case of n odd.

0.8.1 Summary of the main contributions

Our main contributions is to study the link between the semi-bentness property of certain classes of Boolean functions and some classical (binary) exponential sums as well as the construction of more semi-bent functions with an even number of variables. In a first work, we have extensively investigated the link between the semi-bentness property of functions in univariate forms obtained via Dillon and Niho functions and Kloosterman sums [201]. In particular, we have showed that zeros and the value four of binary Kloosterman sums give rise to semi-bent functions in even dimension with maximum degree. Moreover, we have studied the semi-bentness property of functions in polynomial forms with multiple trace terms and exhibit criteria involving Dickson polynomials. Next, we have reformulated the characterizations in terms of cardinalities of hyper-elliptic curves in order to obtain efficient ones [9]. Our study on the explicit constructions of families of semi-bent functions allowed us to guess that the semi-bent functions whose restriction to the spaces $u\mathbb{F}_{2^m}^\star$ where u ranges the cyclic group of 2^m+1-st of unity are essentially the functions obtained by adding a bent function of Niho type and a function in the $\mathcal{PS}_{ap}^{\#}$ class.

Following this study, we have generalized in a joint work with Carlet the constructions of semi-bent functions proposed in [199] and we have showed in [45] how to construct semi-bent Boolean functions in even dimension from a $\mathcal{PS}_{ap}$-like bent function g and a bent function h whose restrictions to the elements of the spread used for defining g are all linear that is, an element of class H. Given a spread $(E_i)_{i=1,\ldots,2^m+1}$, we have characterized when a function whose restriction to every E_i^* is affine (i.e. a function equal to the sum of a function whose restriction to every E_i is linear and of a function whose restriction to every E_i^* is constant) is semi-bent:

Theorem 0.8.1. *Let $m \geq 2$ and $n = 2m$. Let $\{E_i,\, i = 1, \ldots, 2^m+1\}$ be a spread in $\mathbb{F}_{2^n}$ and h a Boolean function whose restriction to every E_i is linear (possibly null). Let S be any subset of $\{1, \ldots, 2^m+1\}$ and $g = \sum_{i\in S} 1_{E_i} \pmod 2$ where 1_{E_i} is the indicator of E_i. Then $g+h$ is semi-bent if and only if g and h are bents. (We call g a $\mathcal{PS}_{ap}$-like bent function)*

From Theorem 0.8.1 and thanks to our results with Carlet on the class $\mathcal{H}$ (see Chapter 4), we have deduced a large number of infinite classes of semi-bent functions in explicit bivariate polynomial form. We have obtained, for every choice of a balanced function over $\mathbb{F}_{2^{n/2}}$, eight new families in bivariate form using the infinite classes of bent functions in bivariate form from Dillon's class $H($ [44]), which have been recently found:

Let g be a function in the $\mathcal{PS}_{ap}$ class. Let h be one of the following functions ([44]) :

- $h(x,y) = \mathrm{Tr}_1^m(x^{-5}y^6)$, m odd;
- $h(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$, m odd:
- $h(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$, $m = 4k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$, $m = 4k-1$;

[9] In fact, this was our first work done in the spirit of Lisonek's approach.

- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^{2k+1}-2^{3k+1}} y^{2^{2k+1}+2^{3k+1}})$, $m = 4k+1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{2^{3k+1}-2^{2k+1}+2^k} y^{1-2^{3k+1}+2^{2k+1}-2^k})$, $m = 4k+1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^k} y^{2^k} + x^{-(2^k+1)} y^{2^k+2} + x^{-3\cdot(2^k+1)} y^{3\cdot 2^k+4})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(y(y^{2^k+1}x^{-(2^k+1)} + y^3 x^{-3} + yx^{-1})^{2^{k-1}-1})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}} y^{\frac{1}{6}} + x^{\frac{1}{2}} y^{\frac{1}{2}} + x^{\frac{1}{6}} y^{\frac{5}{6}})$, m odd;
- $h(x,y) = \mathrm{Tr}_1^m(x[D_{\frac{1}{5}}\left(\frac{y}{x}\right)]^6)$, m odd, where $D_{\frac{1}{5}}$ is the Dickson polynomial of index $\frac{1}{5}$.

Then the function $g+h$ is semi-bent.

Secondly, in the framework where the functions are considered in their univariate form, we have applied Theorem 0.8.1 to the spread $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ (where U is the multiplicative group $\{u \in \mathbb{F}_{2^n}; u^{2^m+1} = 1\}$). In this case, on one hand, nonlinear Boolean functions whose restriction to any vector space $u\mathbb{F}_{2^m}$ are linear are sums of Niho power functions, that is (see [93]) of functions of the form:

$$\mathrm{Tr}_1^{o((2^m-1)s+1)}\left(a_s x^{(2^m-1)s+1}\right) \text{ with } 1 \le s \le 2^m$$

On the other hand, some $\mathcal{PS}_{ap}$ functions can be obtained in the form

$$\sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}\left(b_r x^{(2^m-1)r}\right) \text{ where } R \subset \{1,\cdots,2^m\}.$$

Collecting results provided by Dobbertin et al. in [93] and by Charpin and Gong in [54], we have obtained the following result:

Corollary 0.8.2. *Let f be a Boolean function of the form:*

$$f(x) = \mathrm{Tr}_1^m(a_0 x^{2^m+1}) + \sum_{i=1}^{L} \mathrm{Tr}_1^n(a_i x^{(2^m-1)s_i+1}) + \sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}(b_r x^{(2^m-1)r})$$

where L is some non-negative integer, $2 \le s_i \le 2^m$, $s_i \ne 2^{m-1}+1$, $1 \le r \le 2^m$, $a_0 \in \mathbb{F}_{2^m}$, $a_i \in \mathbb{F}_{2^m}$ and $b_r \in \mathbb{F}_{2^{o((2^m-1)r)}}$ (with at least one coefficient $a_i \ne 0$ and one coefficient $b_r \ne 0$). Assume that:
1) the number of roots u in $U := \{x \in \mathbb{F}_{2^n}; x^{2^m+1} = 1\}$ of the equation $\mathrm{Tr}_m^n(cu) + \sum_{i=1}^{L} \mathrm{Tr}_m^n(a_i u^{2s_i-1}) + a_0^{\frac{1}{2}} = 0$ is either 0 or 2 for every $c \in \mathbb{F}_{2^n}$,
2) the sum $\sum_{u\in U} \chi(\sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}(b_r u^r))$ is equal to 1. Then, f is semi-bent.

Thanks to the previous result and our results on hyper-bent functions, we have therefore derived at least thirty new infinite classes of semi-bent functions $g_i + h_j$ ($i \in \{1,\cdots,6\}$, $j \in \{1,\cdots,5\}$) in univariate form where g_i belongs to the following list of infinite families containing bent functions defined on $\mathbb{F}_{2^n}$ in the class $\mathcal{PS}_{ap}$:

- $g_1(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)})$; $\gcd(r, 2^m+1) = 1$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 0$
- $g_2(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$; $\gcd(r, 2^m+1) = 1$, $m > 3$ odd, $b \in \mathbb{F}_4^\star$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$
- $g_3(x) = \mathrm{Tr}_1^n(a\zeta^i x^{3(2^m-1)}) + \mathrm{Tr}_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th of unity, $(i,j) \in \{0,1,2\}^2$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$ and $\mathrm{Tr}_1^m(a^{1/3}) = 0$

- $g_4(x) = \mathrm{Tr}_1^n(a\zeta^i x^{3(2^m-1)}) + \mathrm{Tr}_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th of unity, $i \in \{1,2\}$, $j \in \{0,1,2\}$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) + C_m(a,a) = 4$ and $\mathrm{Tr}_1^m(a^{1/3}) = 1$,
- $g_5(x) = \sum_{i=1}^{2^{m-1}-1} \mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$; $\beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$,
- $g_6(x) = \sum_{i=1}^{2^{m-2}-1} \mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$; m odd and $\beta^{(2^m-4)^{-1}} \in \{x \in \mathbb{F}_{2^m}^\star; \mathrm{Tr}_1^m(x) = 0\}$,

and h_j belongs to the following list of known Niho bent functions:

- $h_1(x) = \mathrm{Tr}_1^m\left(a_1 x^{2^m+1}\right)$; $a_1 \in \mathbb{F}_{2^m}^\star$
- $h_2(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)3+1}\right)$;
  $a_1 \in \mathbb{F}_{2^n}^\star$, $a_2^{2^m+1} = a_1 + a_1^{2^m} = \beta^5$ for some $\beta \in \mathbb{F}_{2^n}^\star$
- $h_3(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{4}+1}\right)$;
  $a_1 \in \mathbb{F}_{2^n}^\star$ $a_2^{2^m+1} = a_1 + a_1^{2^m}$, m odd
- $h_4(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{6}+1}\right)$; $a_1 \in \mathbb{F}_{2^n}^\star$ $a_2^{2^m+1} = a_1 + a_1^{2^m}$, m even
- $h_5(x) = \mathrm{Tr}_1^n\left(\alpha x^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} x^{s_i}\right)$, $r > 1$ such that $gcd(r,m) = 1$, $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha + \alpha^{2^m} = 1$, $s_i = (2^m-1)\frac{i}{2^r} \pmod{2^m+1} + 1$, $i \in \{1, \cdots, 2^{r-1}-1\}$

0.8.2 Publications

The results presented in this chapter have been the subject of the following publications:

- S. Mesnager. Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. IEEE Transactions on Information Theory-IT, Vol 57, No 11, pages 744–7458, 2011([199]).
- S. Mesnager. Semi-bent functions with multiple trace terms and hyperelliptic curves. Proceeding of International Conference on Cryptology and Information Security in Latin America (IACR), Latincrypt 2012, LNCS 7533, Springer, pages 18–36, 2012 ([200]).
- S. Mesnager and G. Cohen . On the link of some semi-bent functions with Kloosterman sums. Proceeding of International Workshop on Coding and Cryptology (IWCC 2011), LNCS 6639, pages 263–272, Springer, 2011([201]).
- C. Carlet and S. Mesnager. On Semi-bent Boolean Functions. IEEE Transactions on Information Theory-IT, Vol 58, No 5, pages 3287-3292, 2012 ([45]).

0.9 Chapter 9

Reed-Muller codes, introduced by D. E. Muller and L. S. Reed in 1954, are one of the best understood families of codes. Except for first-order Reed-Muller codes and for codes of small lengths, their minimum distance is lower than that of BCH codes. But they have very efficient decoding algorithms, they contain nonlinear sub-codes with optimal parameters together with efficient decoding algorithms, and they give a useful framework for the study of Boolean functions in cryptography. Despite the fact that they have been extensively studied for decades by

coding theorists, their covering radius is unknown except for Reed-Muller codes of small lengths and for the first-order Reed-Muller code of length 2^n, for n even. The covering radius is the smallest integer ρ such that the spheres of radius ρ centered at the codewords cover the whole space, i.e. the maximum multiplicity of errors that have to be corrected when maximum likelihood decoding is used on a binary symmetric channel. Lower and upper bounds have been proved, but the gap between them is important, and better bounds have to be found. A good reference on covering radius is [68] and a short non-exhaustive list of references on this subject is [69, 130, 131, 186, 230, 239].

Reed-Muller codes can be defined in terms of Boolean functions. Precisely, the binary r^{th}-order Reed-Muller code $RM(r,n)$ is the set of all binary vectors of length 2^n associated with multivariate binary polynomials $f(x_1,\ldots,x_n)$ of algebraic degree at most r. The covering radius[10] of $\mathcal{RM}(r,n)$ coincides with the maximal nonlinearity of order r of Boolean functions. The nonlinearity of order r generalizes the standard nonlinearity and is thus an important parameter in cryptography, which equals the maximum distance between any Boolean function f and $\mathcal{RM}(r,n)$ and measures the capacity for resisting low-degree approximation attacks [152, 234]. In [152], the techniques exposed pose a threat even when Matsui's advanced linear cryptanalytic attacks are rendered impractical. The nonlinearity of order r has also some relationship with algebraic attacks [73, 187], as shown in [34], which rely on the existence of low-degree relations between the input and the output to the involved function which rely on the existence of low-degree annihilators of the function or its complement.

0.9.1 Summary of the main contributions

By deriving bounds on character sums of Boolean functions and by using the characterizations, due to Kasami and Tokura, of those elements of the Reed-Muller codes whose Hamming weights are smaller than twice and a half the minimum distance, we derive an improved upper bound on the covering radius $\rho(2,n)$ of the second-order Reed-Muller code $\mathcal{RM}(2,n)$.

The best upper bound on the covering radius $\rho(2,m)$ is given by the following theorem[43].

Theorem 0.9.1. *(9.1.1) For every positive integer $n \geq 17$, the covering radius $\rho(2,n)$ of the second-order Reed-Muller code $\mathcal{RM}(2,n)$ is upper bounded by*

$$\left\lfloor 2^{n-1} - \frac{\sqrt{15}}{2} \cdot 2^{\frac{n}{2}} \cdot \left(1 - \frac{122929}{21 \cdot 2^n} - \frac{155582504573}{4410 \cdot 2^{2n}}\right)\right\rfloor \tag{7}$$

The best known asymptotic upper bound on the covering radius $\rho(r,m)$ of the Reed-Muller code of order r, $r \geq 2$, is:

$$\rho(2,n) \leq 2^{n-1} - \sqrt{15}\, 2^{\frac{n}{2}-1} + O(1).$$

Consequently, by induction on r, we deduce improved upper bounds on the covering radii of the Reed-Muller codes of higher orders.

Theorem 0.9.2. *(9.1.2) Let r be a positive integer greater than or equal to 2. The covering radius of the Reed-Muller code of order r satisfies asymptotically*

$$\rho(r,n) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{n/2} + O(n^{r-2}) \tag{8}$$

[10]Note that in the context of some stream ciphers, a notion of covering radius considering the distance between resilient functions and binary Reed-Muller codes has also been proposed in [143, 7].

Our results have improved the best known upper bounds dating 15 years. Up to now, our bounds are the best bounds known in the literature.

In the following we give the outline of our method which allows as to improve the upper bound $\rho(2,m)$. The first idea was to introduce the following sums:

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}. \tag{9}$$

Next, we have proved that the covering radius $\rho(2,m)$ satisfies

$$\forall k \geq 1, \quad \rho(2,m) \leq 2^{m-1} - \frac{1}{2} \min_{f \in \mathcal{B}_m} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \tag{10}$$

Moreover, we have proved that for any Boolean function $f \in \mathcal{B}_m$, we have

$$\begin{aligned}
&\mathcal{S}_k(f) = \#\,\mathcal{RM}(2,m)\, D_k \quad \text{if } k = 1,2,3 \\
&\mathcal{S}_k(f) \#\,\mathcal{RM}(2,m) \left(D_k + N_k^{(8)} M_f^{(8)} \right) \text{if } k = 4,5 \\
&\mathcal{S}_k(f) = \#\,\mathcal{RM}(2,m) \left(D_k + N_k^{(8)} M_f^{(8)} + \sum_{w=6}^{k} 2wk M_f^{(2w)} \right) \text{if } k \geq 6
\end{aligned}$$

with

- D_k be the number of ways of choosing a $2k$-tuple $(x_1, \cdots, x_{2k})$ such that $\sum_{i=1}^{2k} 1_{x_i}$ equals the null codeword.
- $N_k^{(w)} = \#\mathcal{N}_g$ whenever $\mathrm{wt}(g) = w$ where $\mathcal{N}_g$ denotes the set of all the $2k$-tuples $(x_1, \ldots, x_{2k})$ of vectors of $\mathbb{F}_2^m$ such that $\sum_{i=1}^{2k} 1_{x_i} = g$.
- $M_f^{(w)}$ be the character sum of $(-1)^{\langle f,g \rangle}$ when g ranges over the subset of those codewords of to the dual code $\mathcal{RM}(2,m)^{\perp}$ of the second-order Reed-Muller code, that is the Reed-Muller code $\mathcal{RM}(m-3,m)$ of order $m-3$ of Hamming weight w.

The values of the numbers D_k and $N_k^{(w)}$ can be computed thanks to the following formulas (given a mapping A from $\mathbb{R}$ to itself, we denote by $\left[z^k\right] A(z)$ the coefficient of $\frac{z^k}{k!}$ in the Taylor series expansion of A at $z = 0$):

$$D_k = [z^{2k}] \cosh^{2^n}(z)$$

$$N_k^{(2w)} = [z^{2k}] \tanh^{2w} \cosh^{2^n}(z)$$

Now, getting an upper bound on $\rho(2,m)$ is equivalent to searching a lower bound of $min_{f \in \mathcal{B}_m} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$. To this end, we have used the characterizations of the elements of the Reed-Muller code $\mathcal{RM}(m-3,m)$.

0.9.2 Publications

The first results of our method were published at the International conference ISIT. The completion of this work has led to a publication at IEEE-IT:

- C. Carlet and S. Mesnager. "Improving the upper bounds on the covering radii of binary Reed-Muller codes". IEEE Transactions on Information Theory, vol. 53, no. 1, pages, 162–173, 2007([43]).

Part I

Boolean Functions

Chapter 1

Generalities on Boolean functions

Contents

1.1 Background on Boolean functions

In mathematics, a Boolean function f is a map from the vectorspace $\mathbb{F}_2^n$ of all binary vectors of length n to the finite field with two elements $\mathbb{F}_2$ i.e: $f : \mathbb{F}_2^n \to \mathbb{F}_2$.The vectorspace $\mathbb{F}_2^n$ will sometimes be also endowed with the structure of field – the field $\mathbb{F}_{2^n}$ (also denoted by $\mathbb{F}_{2^n}$); indeed, this field being an n-dimensional vectorspace over $\mathbb{F}_2$, each of its elements can be identified with the binary vector of length n of its coordinates relative to a fixed basis. The set of all Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ will be denoted by $\mathcal{B}_n$. The *Hamming weight* $\mathrm{wt}(x)$ of a binary vector $x \in \mathbb{F}_2^n$ being the number of its nonzero coordinates (*i.*e. the size of $\{i \in N/\ x_i \neq 0\}$ where N denotes the set $\{1, \cdots, n\}$, called the *support* , the *Hamming weight of a Boolean function* f on $\mathbb{F}_2^n$ is denoted by $\mathrm{wt}(f)$ is (also) the size of the support of the function , *i.e.* the set $\{x \in \mathbb{F}_2^n/\ f(x) \neq 0\}$. The *Hamming distance* $d_H(f, g)$ between two functions f and g is the size of the set $\{x \in \mathbb{F}_2^n/\ f(x) \neq g(x)\}$. Thus it equals $w_H(f \oplus {}^1 g)$.

Boolean functions play an important role in both cryptographic and error correcting coding activities. Indeed, cryptographic transformations (pseudo-random generators in stream ciphers, S-boxes in block ciphers) can be designed by appropriate composition of nonlinear Boolean functions. Moreover, every code of length 2^n, for some positive integer n, can be interpreted as

[1] Some additions of bits will be considered in $\mathbb{Z}$ (in characteristic 0) and denoted then by $+$, and some will be computed modulo 2 and denoted by $\oplus$ or by $+$ if there is no ambiguity. These two different notations will be necessary because some representations of Boolean functions will live in characteristic 2 and some representations of the same functions will live in characteristic 0. But the additions of elements of the finite field $\mathbb{F}_{2^n}$ will be denoted by $+$, as it is usual in mathematics. So, for simplicity (since $\mathbb{F}_2^n$ will often be identified with $\mathbb{F}_{2^n}$) and because there will be no ambiguity, we shall also denote by $+$ the addition of vectors of $\mathbb{F}_2^n$ when $n > 1$.

a set of Boolean functions, since every n-variable Boolean function can be represented by its truth table (an ordering of the set of binary vectors of length n being first chosen) and thus associated with a binary word of length 2^n, and *vice versa*; important codes such as Reed-Muller and Kerdock codes can be defined this way as sets of Boolean functions.

In both frameworks, n is rarely large, in practice. The error correcting codes derived from n-variable Boolean functions have length 2^n; so, taking $n = 11$ already gives codes of length 2048. For reason of efficiency, the S-boxes used in most block ciphers are concatenations of sub S-boxes on at most 8 variables. In the case of stream ciphers, n was in general at most equal to 11 until recently. The cryptographic situation has changed a little in practice since the apparition of the algebraic attacks but the number of variables is now most often limited to 20. An excellent reference for Boolean functions is the Book's chapter of Claude Carlet ([31], Chapter 8).

1.2 Boolean functions: representations

There exist several representations of a given Boolean function. We shall recall only the representations of Boolean functions that we need in this manuscript.

1.2.1 Algebraic normal Form

The algebraic normal Form (in brief the ANF) is the classical representation of Boolean functions. It is the one which is the most usually used in cryptography and coding. The Algebraic Normal Form of an Boolean function f on $\mathbb{F}_2^n$ is the n-variable polynomial representation over $\mathbb{F}_2$, of the form

$$f(x) = \bigoplus_{I \in \mathcal{P}(N)} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{I \in \mathcal{P}(N)} a_I \, x^I, \tag{1.1}$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, \cdots, n\}$. Every coordinate x_i appears in this polynomial with exponents at most 1, because every bit in $\mathbb{F}_2$ equals its own square. This representation belongs to $\mathbb{F}_2[x_1, \cdots, x_n]/(x_1^2 \oplus x_1, \cdots, x_n^2 \oplus x_n)$.

The *algebraic degree* of the function f (this makes sense thanks to the existence and uniqueness of the ANF) denoted by $\deg(f)$ equals the maximum degree of those monomials whose coefficients are nonzero in its algebraic normal form, that is, $\deg(f) = \max\{|I| / \, a_I \neq 0\}$, where $|I|$ denotes the size of I.

The algebraic degree is an affine invariant (it is invariant under the action of the general affine group).

1.2.2 Numerical normal form

Any n-variable Boolean function can be viewed as an integer-valued mapping taking values in the subset $\{0, 1\}$ of $\mathbb{Z}$. Now, any integer-valued mapping f can be uniquely represented as a multivariate polynomial over $\mathbb{Z}$:

$$\forall x \in \mathbb{F}_2^n, \quad f(x) = \sum_{I \in \mathcal{P}_n} \lambda_I \prod_{i \in I} x_i \tag{1.2}$$

where the λ_I's are in $\mathbb{Z}$. This representation is unique and called the *numerical normal form*[2]. The degree of the numerical normal form of an integer-valued map f is called its *numerical*

[2]This representation has been introduced by Carlet and Guillot in [38] in the framework of cryptography.

degree. To ensure that f takes values in $\{0,1\}$, that is, satisfies $f^2(x) = f(x)$ for every $x \in \mathbb{F}_2^n$, the coefficients λ_I's have to satisfy

$$\forall I \in \mathcal{P}_n, \quad \Big(\sum_{J\subset I} \lambda_J\Big)^2 - \sum_{J\subset I} \lambda_J \;=\; 0. \tag{1.3}$$

where $\sum_{J\subset I}$ denotes the summation over all the subsets J of $\{1,\ldots,n\}$ which are contained in the subset I.

Note that the numerical normal form leads to a (simple) characterization of the bent functions[3] [39].

1.2.3 Trace function and the polynomial form

Now, we consider a Boolean function f defined on $\mathbb{F}_{2^n}$, that is, is an $\mathbb{F}_2$-valued function on the Galois field $\mathbb{F}_{2^n}$ of order 2^n. The weight *of f, denoted by* $\mathrm{wt}(f)$*, is the Hamming weight of the image vector of f, that is, the cardinality of its support $\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.*

For any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$ is denoted by $\mathrm{Tr}_r^k(\cdot)$. It can be defined as

$$\mathrm{Tr}_r^k(x) = \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}} \quad .$$

In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Recall some basic properties of trace functions:

1. the trace function Tr_k^n is surjective;
2. $\mathrm{Tr}_k^n(ax+by) = a\,\mathrm{Tr}_k^n(x) + b\,\mathrm{Tr}_k^n(y)$ for $a,b \in \mathbb{F}_{2^k}$ and $x,y \in \mathbb{F}_{2^n}$;
3. $\mathrm{Tr}_k^n(x^{2^k}) = \mathrm{Tr}_k^n(x)$ for $x \in \mathbb{F}_{2^n}$;
4. when $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^r} \subset \mathbb{F}_{2^n}$, the trace function Tr_k^n satisfies the transitivity property, that is, $\mathrm{Tr}_k^n = \mathrm{Tr}_k^r \circ \mathrm{Tr}_r^n$.

There exist several kinds of possible trace (univariate) representations of Boolean functions (see for instance, [31], page 266) which are not necessary unique and use the identification between the vector-space $\mathbb{F}_2^n$ and the field $\mathbb{F}_{2^n}$. In this manuscript, we will extensively study the so-called *Bent functions*. Those functions are often better viewed in their bivariate representation and can also be viewed in their univariate representation. The univariate representation of any Boolean function is defined as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ (which is an n-dimensional vector space over $\mathbb{F}_2$) and we consider then the input to f as an element of $\mathbb{F}_{2^n}$. An inner product in $\mathbb{F}_{2^n}$ is $x \cdot y = \mathrm{Tr}_1^n(xy)$ where $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. There exists a unique univariate polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ over $\mathbb{F}_{2^n}$ such that f is the polynomial function over $\mathbb{F}_{2^n}$ associated to it (this is true for every function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$). Moreover, f being Boolean, its univariate representation can be written as a unique trace expansion of the form

$$f(x) = \sum_{j\in\Gamma_n} \mathrm{Tr}_1^{o(j)}\left(a_j x^j\right) + \epsilon(1 + x^{2^n-1}), \quad a_j \in \mathbb{F}_{2^{o(j)}} \quad ,$$

valid for all $x \in \mathbb{F}_{2^n}$ and called its *polynomial form*. In the above expression:

[3] The definition of a bent function is given later in Chapter 4.

1. Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset modulo $2^n - 1$ (including the trivial coset containing 0 and only 0), the most usual choice being the smallest element in each cyclotomic coset, called the coset leader,

2. $o(j)$ is the size of the cyclotomic coset containing j (that is, $o(j)$ is the smallest positive integer such that $j2^{o(j)} \equiv j \pmod{2^n - 1}$),

3. and $\epsilon = \mathrm{wt}(f) \pmod 2$.

The *algebraic degree* of f is then equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$. Recall that the 2-weight $w_2(j)$ of an integer j is equal to the number of 1's in its binary expansion[4].

Note that the above expression of f can also be written under a non-unique form $\mathrm{Tr}_1^n(P(x))$ where $P(x)$ is a polynomial over $\mathbb{F}_{2^n}$.

Going from the non-unique trace representation to the unique one basically amounts to take the traces of the coefficients from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{o(j)}}$. Going the other way around relies on the surjectivity of the trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{o(j)}}$.

1.2.4 The bivariate representation

The *bivariate representation* of Boolean functions is defined only when $n = 2m$ is even as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and we consider then the input to f as an ordered pair (x, y) of elements of $\mathbb{F}_{2^m}$. There exists a unique bivariate polynomial

$$\sum_{0 \leq i,j \leq 2^m - 1} a_{i,j} x^i y^j$$

over $\mathbb{F}_{2^m}$ such that f is the bivariate polynomial function over $\mathbb{F}_{2^m}$ associated to it. Then the algebraic degree of f equals

$$\max_{(i,j) \mid a_{i,j} \neq 0} (w_2(i) + w_2(j)).$$

And f being Boolean, its bivariate representation can be written in the form

$$f(x, y) = \mathrm{Tr}_1^m(P(x, y))$$

where $P(x, y)$ is some polynomial in two variables over $\mathbb{F}_{2^m}$.

[4]More precisely, for $j \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$, $w_2(j)$ is the Hamming (or binary) weight of the unique representative of j in $\{0, \ldots, 2^k - 2\}$.

Chapter 2

Some mathematical tools

Contents

2.1 Walsh Hadamard transform

Let $\chi : \mathbb{F}_2 \mapsto \mathbb{Z}$ denote the nontrivial additive character of $\mathbb{F}_2$. The *"sign" function* of a Boolean function f is the integer-valued function $\chi_f = \chi(f)$ that is, $\chi_f = (-1)^f$.

Let f be a Boolean function defined on $\mathbb{F}_2^n$. Then the *Walsh Hadamard transform* of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_2^n$ is defined as follows:

$$\forall \omega \in \mathbb{F}_2^n, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x}.$$

(that is, $\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_2^n} \chi(f(x) + \omega \cdot x)$) where "$\cdot$" is the scalar product in $\mathbb{F}_2^n$ defined as $x \cdot y = \sum_{i=1}^n x_i y_i$.

The notion of Walsh transform refers to a scalar product[1]. When $\mathbb{F}_2^n$ is identified with the field $\mathbb{F}_{2^n}$ by an isomorphism between these two n-dimensional vector spaces over $\mathbb{F}_2$, it is convenient to choose the isomorphism such that the canonical scalar product " $\cdot$ " in $\mathbb{F}_2^n$ coincides with the canonical scalar product in $\mathbb{F}_{2^n}$, which is the trace of the product : $x \cdot y = \sum_{i=1}^n x_i y_i = \mathrm{Tr}_1^n(xy)$ for $x, y \in \mathbb{F}_{2^n}$. Thus if f is a Boolean function defined on $\mathbb{F}_{2^n}$ then, the Walsh Hadamard transform

[1]Note that in the definition of the Walsh transform, we can take any inner product; the cryptographic properties are not related to a particular choice of the inner product therefore, the issue of the choice of the isomorphism does not arise.

of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as follows:

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\omega x)}.$$

(that is, $\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} \chi\left(f(x) + \mathrm{Tr}_1^n(\omega x)\right)$). .

The Walsh transform satisfies the well-known Parseval's relation

$$\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}^2(\omega) = 2^{2n}$$

and also the inverse Fourier formula

$$\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}(\omega) = 2^n (-1)^{f(0)}.$$

Note that not all values of the Walsh Hadamard transform can have the same sign, except when the function is affine. This comes from the fact that we then have $\left(\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}(\omega)\right)^2 = \sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}^2(\omega)$ which implies that all these values are null except one.

Now, let f be a Boolean function on $\mathbb{F}_{2^n}$. Then the *extended Walsh-Hadamard transform* of f is defined as.

$$\widehat{\chi_f}(\omega, k) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n\left(\omega x^k\right)} \ ,$$

for $\omega \in \mathbb{F}_{2^n}$ and k an integer co-prime with $2^n - 1$.

2.2 Some classical binary exponential sums

2.2.1 Binary Kloosterman sums

Binary *Kloosterman sums* are widely studied for a long time for their own sake as interesting mathematical objects and have recently become the focus of much research, most notably due to their applications in cryptography and for their connection to coding theory. The classical binary Kloosterman sums on $\mathbb{F}_{2^m}$ (where m is an arbitrary positive integer) are defined as follows.

Definition 2.2.1. *Let $a \in \mathbb{F}_{2^m}$. The binary Kloosterman sums on $\mathbb{F}_{2^m}$ associated with a is*

$$K_m(a) := \sum_{x \in \mathbb{F}_{2^m}} \chi\big(\mathrm{Tr}_1^m(ax + \frac{1}{x})\big), \quad a \in \mathbb{F}_{2^m}$$

The Kloosterman sums are generally defined on the multiplicative group $\mathbb{F}_{2^m}^\star$ of $\mathbb{F}_{2^m}$. In the document we extend to 0 assuming that $\chi(\mathrm{Tr}_1^m(\frac{1}{x})) = 1$ for $x = 0$ (in fact, $\mathrm{Tr}_1^m(\frac{1}{x}) = \mathrm{Tr}_1^m(x^{2^{m-1}-1})$).

In particular, such exponential sum can be seen as the Walsh–Hadamard transform of a simple function. Indeed, the function $a \mapsto K_n(a)$ is the Walsh–Hadamard transform of the inverse function (we define $1/0 = 0$ or $1/x$ as x^{2^n-2} for all $x \in \mathbb{F}_{2^n}$).

It is an elementary fact that $K_n(a) = K_n(a^2)$. Indeed,

$$K_n(a) = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(ax+\frac{1}{x}\right)} = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(a^2x^2+\frac{1}{x^2}\right)}$$
$$= 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_1^n\left(a^2x+\frac{1}{x}\right)} = K_n(a^2) \ .$$

The following proposition is directly obtained from the result of Lachaud and Wolfmann in [156] which is suitable for any arbitrary positive integer m.

Proposition 2.2.2. *([156]) Let m be a positive integer. The set $\{K_m(a), a \in \mathbb{F}_{2^m}\}$, is the set of all the integers multiple of 4 in the range $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$.*

Divisibility properties of the Kloosterman sums have been studied in several recent papers. Recall, in particular, the following result given by Charpin, Helleseth and Zinoviev in [61] on the divisibility by 3 of $K_m(a) - 1$.

Proposition 2.2.3. *([61]) Let $m \geq 3$ be an odd integer, and let $a \in \mathbb{F}_{2^m}^\star$. Then,*

$$K_m(a) - 1 \equiv 0 \pmod 3 \Longleftrightarrow \mathrm{Tr}_1^m(a^{1/3}) = 0$$

2.2.2 Binary cubic sums

The binary cubic sums on $\mathbb{F}_{2^m}$ (where m is an arbitrary positive integer) are defined as follows.

Definition 2.2.4. *The cubic sums on $\mathbb{F}_{2^m}$ are:*

$$C_m(a,b) := \sum_{x \in \mathbb{F}_{2^m}} \chi\big(\mathrm{Tr}_1^m(ax^3+bx)\big), \quad a \in \mathbb{F}_{2^m}^\star, b \in \mathbb{F}_{2^m}$$

Of course, such exponential sum can be seen as the Walsh–Hadamard transform of a simple function. Indeed, the function $b \mapsto C_m(a,b)$ is the Walsh–Hadamard transform of the cube function times a defined as $x \mapsto ax^3$.

The exact values of the cubic sums $C_m(a,a)$ on $\mathbb{F}_{2^m}$ can be computed thanks to Carlitz's result [52] by means of the Jacobi symbol. Recall that the Jacobi symbol $\left(\frac{2}{m}\right)$ is a generalization of the Legendre symbol (which is defined when m is an odd prime). For m odd, $\left(\frac{2}{m}\right) = (-1)^{\frac{(m^2-1)}{8}}$.

Proposition 2.2.5. *([52]) Let m be an odd integer. Then we have:*

1. $C_m(1,1) = \left(\frac{2}{m}\right) 2^{(m+1)/2}$,
2. *If $\mathrm{Tr}_1^m(c) = 0$, then $C_m(1,c) = 0$,*
3. *If $\mathrm{Tr}_1^m(c) = 1$ (with $c \neq 1$), then $C_m(1,c) = \chi(\mathrm{Tr}_1^m(\gamma^3+\gamma)) \left(\frac{2}{m}\right) 2^{(m+1)/2}$ where $c = \gamma^4+\gamma+1$ for some $\gamma \in \mathbb{F}_{2^m}$.*

Remark 2.2.6. *Note that when $\mathrm{Tr}_1^m(c) = 1$ and $c \neq 1$, then the cubic sums $C_m(1,c)$ can be computed thanks to a recent result of Charpin et al. in [56]. More precisely, if $\mathrm{Tr}_1^m(c) = 1$ (with $c \neq 1$), then $C_m(1,c) = (-1)^{\mathrm{Tr}_1^m(\gamma^3+\gamma)} \left(\frac{2}{m}\right) 2^{(m+1)/2}$ where γ is the unique element of $\mathbb{F}_{2^m}$ satisfying $c = \gamma^4+\gamma+1$ and $\mathrm{Tr}_1^m(\gamma) = 0$.*

2.2.3 Partial exponential sums

Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. We denote the exponential sum associated with f by $\Xi(f)$, that is

$$\Xi(f) = \sum_{x \in \mathbb{F}_{2^m}} \chi_f(x) \ .$$

With this notation, the classical binary Kloosterman sums associated with a on $\mathbb{F}_{2^m}$ are then defined as

$$K_m(a) = \Xi\left(\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)\right) \ .$$

The following partial exponential sums are a classical tool to study hyper-bentness. Beware that the Boolean function is defined on $\mathbb{F}_{2^n}$ in the first definition and $\mathbb{F}_{2^m}$ in the second one.

Definition 2.2.7. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function and U be the set of (2^m+1)-th roots of unity in $\mathbb{F}_{2^n}$. We define $\Lambda(f)$ as*

$$\Lambda(f) = \sum_{u \in U} \chi_f(u) \ .$$

We define $\mathcal{T}_0$ and $\mathcal{T}_1$ as follows.

Definition 2.2.8. *For $i \in \mathbb{F}_2$, let $\mathcal{T}_i$ denote the set*

$$\mathcal{T}_i = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}_1^m(1/x) = i\} \ .$$

Now, we define the partial exponential sum on $\mathcal{T}_i$ associated with f as follows.

Definition 2.2.9. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function and, for $i \in \mathbb{F}_2$, denote by $T_i(f)$ the partial exponential sum on $\mathcal{T}_i$ associated with f, that is*

$$T_i(f) = \sum_{x \in \mathcal{T}_i} \chi_f(x) \ .$$

The following lemma is easily deduced from the equality $\chi\left(\mathrm{Tr}_1^m(x)\right) = 1 - 2\,\mathrm{Tr}_1^m(x)$ where the values of the trace are understood as the integers 0 and 1.

Lemma 2.2.10. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Then*

$$T_i(f) = \frac{1}{2}\left(\Xi(f) + \chi(i)\,\Xi\left(\mathrm{Tr}_1^m(1/x) + f(x)\right)\right) \ .$$

Finally, we have the following relation between Kloosterman sums and the above partial exponential sums.

Corollary 2.2.11. *Let $a \in \mathbb{F}_{2^m}^*$. Then $K_m(a) = -2T_1(\mathrm{Tr}_1^m(ax)) = 2T_0(\mathrm{Tr}_1^m(ax))$.*

Proof. We have

$$T_0(\mathrm{Tr}_1^m(ax)) - T_1(\mathrm{Tr}_1^m(ax)) = K_m(a) \ .$$

Moreover,

$$T_0(\mathrm{Tr}_1^m(ax)) + T_1(\mathrm{Tr}_1^m(ax)) = \Xi\left(\mathrm{Tr}_1^m(ax)\right) = 0 \ . \qquad \square$$

2.3 Some results on the sum over the cyclic group U of characters

From now, $n = 2m$ is an (even) integer. Recall the well known *polar decomposition*. Let x be an element of $\mathbb{F}_{2^n}$. The conjugate of x over a subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$ will be denoted by $\bar{x} = x^{2^m}$ and the relative norm with respect to the quadratic field extension $\mathbb{F}_{2^n}/\mathbb{F}_{2^m}$ by $norm(x) = x\bar{x}$. Also, we denote by U the set $\{u \in \mathbb{F}_{2^n} \mid norm(u) = 1\} = \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$, which is the group of $(2^m + 1)$-st roots of unity. Since the multiplicative group of the field $\mathbb{F}_{2^n}$ is cyclic and $2^m + 1$ divides $2^n - 1$, the order of U is $2^m + 1$. Finally, the unit 1 is the single element in $\mathbb{F}_{2^m}$ of norm one and every non-zero element x of $\mathbb{F}_{2^n}$ has a unique decomposition as: $x = yu$ with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U$.

In this manuscript, U will always denote the cyclic group of $(2^m + 1)$-st roots of unity that is $\{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$.

In the following we provide several technical results and some mathematical tools that we need subsequently in Chapter 5 and Chapter 8. More precisely, we are interested to express some particular exponential sums over the cyclic group U by means of Kloosterman sums and cubic sums. Such expressions will be useful to exhibit conditions of bentness and semi-bentness (of some Boolean functions in polynomial forms) involving Kloosterman sums and cubic sums.

First we state a well-known result. We give a proof because the result is important.

Proposition 2.3.1. *([156], [84], [159],[56]) Let $n = 2m$, r a positive integer such that $\gcd(r, 2^m + 1) = 1$ and $a \in \mathbb{F}_{2^m}$. Then,*

$$\sum_{u \in U} \chi\left(\mathrm{Tr}_1^n(au^r)\right) = 1 - K_m(a)$$

Proof. Let $a \in \mathbb{F}_{2^m}^\star$. We have

$$K_m(a) = \sum_{x \in \mathbb{F}_{2^m}, \mathrm{Tr}_1^m(1/x)=0} \chi(\mathrm{Tr}_1^m(ax)) - \sum_{x \in \mathbb{F}_{2^m}, \mathrm{Tr}_1^m(1/x)=1} \chi(\mathrm{Tr}_1^m(ax))$$

But

$$\sum_{x \in \mathbb{F}_{2^m}, \mathrm{Tr}_1^m(1/x)=0} \chi(\mathrm{Tr}_1^m(ax)) + \sum_{x \in \mathbb{F}_{2^m}, \mathrm{Tr}_1^m(1/x)=1} \chi(\mathrm{Tr}_1^m(ax)) = \sum_{x \in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^m(ax)) = 0.$$

Hence

$$K_m(a) = -2 \sum_{x \in \mathbb{F}_{2^m}, \mathrm{Tr}_1^m(1/x)=1} \chi(\mathrm{Tr}_1^m(ax))$$

$u \mapsto u + u^{-1}$ is onto and 2-to-1 from $U \setminus \{1\}$ to $\{x \in \mathbb{F}_2 m, \mathrm{Tr}_1^m(1/x) = 1\}$:

$$K_m(a) = -\sum_{u \in U, u \neq 1} \chi(\mathrm{Tr}_1^m(a(u + u^{-1})))$$

But $u + u^{-1} = Tr_m^n(u)$. Thus

$$K_m(a) = -\sum_{u\in U, u\neq 1} \chi(\mathrm{Tr}_1^n(au) = -\sum_{u\in U} \chi(\mathrm{Tr}_1^n(au) + 1$$

Now, it is clear that for r coprime with 2^m+1 we have, $\sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au^r)\right) = \sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au)\right)$. □

The following result extends Proposition 2.3.1.

Proposition 2.3.2. *([199]) Let $n = 2m$ with m odd. Let $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4^\star$ and r a positive integer such that $\gcd(r, 2^m+1) = 1$. Then,*

$$\sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au^r) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right) = \frac{K_m(a) - 1 + \lambda C_m(a,a)}{3}$$

where $\lambda = 4$ if $b = 1$ and $\lambda = -2$ otherwise.

Proof. Set $S(a,b) := \sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au^r) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right)$. The mapping $u \mapsto u^r$ is a permutation of U (we denote by $x \mapsto x^{\frac{1}{r}}$ its inverse map) since $gcd(r, 2^m+1) = 1$. Hence, $S(a,b) = \sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(au) + \mathrm{Tr}_1^2(bu^{\frac{1}{r}\frac{2^m+1}{3}})\right)$. Now, m being odd, we have the the following decomposition of U:

$$U = V \cup \zeta V \cup \zeta^2 V$$

where $V := \{u^3 \mid u \in U\}$ and ζ is a generator of the cyclic group U. Therefore,

$$\begin{aligned} S(a,b) &= \sum_{j=0}^{2} \sum_{v\in V} \chi\left(\mathrm{Tr}_1^n(a\zeta^j v) + \mathrm{Tr}_1^2(b\zeta^{\frac{j}{r}\frac{2^m+1}{3}})\right) \\ &= \sum_{j=0}^{2} \sum_{v\in V} \chi\left(\mathrm{Tr}_1^n(a\zeta^j v)\right) \chi\left(\mathrm{Tr}_1^2(b\zeta^{\frac{j}{r}\frac{2^m+1}{3}}))\right) \\ &= \sum_{j=0}^{2} \chi\left(\mathrm{Tr}_1^2(b\zeta^{\frac{j}{r}\frac{2^m+1}{3}})\right) \sum_{v\in V} \chi\left(\mathrm{Tr}_1^n(a\zeta^j v)\right). \end{aligned}$$

For $j \in \{0,1,2\}$, set

$$\sigma_j(a) := \sum_{v\in V} \chi(\mathrm{Tr}_1^n(a\zeta^j v)).$$

Then we have

$$S(a,b) = \sum_{j=0}^{2} \chi(\mathrm{Tr}_1^2(b\zeta^{\frac{j}{r}\cdot\frac{2^m+1}{3}}))\sigma_j(a).$$

Remark that, for every $a \in \mathbb{F}_{2^m}$, $\sigma_1(a) = \sigma_2(a)$. Indeed, ζ^{2^m-2} is an element of V because 3 divides (2^m+1) (since m is odd) and the mapping $v \mapsto \zeta^{2^m-2}v^{2^m}$ is a permutation on V. Then,

$$\begin{aligned} \sigma_1(a) &= \sum_{v\in V} \chi(\mathrm{Tr}_1^n(a\zeta v)) = \sum_{v\in V} \chi(\mathrm{Tr}_1^n(a\zeta^{2^m} v^{2^m})) \\ &= \sum_{v\in V} \chi(\mathrm{Tr}_1^n(a\zeta^2(\zeta^{2^m-2}v^{2^m}))) = \sigma_2(a). \end{aligned}$$

Hence,

$$S(a,b) = \chi(\mathrm{Tr}_1^2(b))\sigma_0(a) + \left(\chi(\mathrm{Tr}_1^2(b\zeta^{\frac{1}{r}\cdot\frac{2^m+1}{3}})) + \chi(\mathrm{Tr}_1^2(b\zeta^{\frac{2}{r}\cdot\frac{2^m+1}{3}}))\right)\sigma_1(a).$$

Now, note that since ζ is a generator element of U, $\mathrm{Tr}_1^2(\zeta^{\frac{1}{r}\cdot\frac{2^m+1}{3}}) = \mathrm{Tr}_1^2(\zeta^{\frac{2}{r}\cdot\frac{2^m+1}{3}}) = 1$. Moreover, if $b \in \mathbb{F}_4^\star \setminus \{1\}$ then, $\chi(\mathrm{Tr}_1^2(b\zeta^{\frac{1}{r}\cdot\frac{2^m+1}{3}})) + \chi(\mathrm{Tr}_1^2(b\zeta^{\frac{2}{r}\cdot\frac{2^m+1}{3}})) = 0$.

Therefore,

$$S(a,b) = \begin{cases} \sigma_0(a) - 2\sigma_1(a) & \text{if } b = 1 \\ -\sigma_0(a) & \text{if } b \neq 1 \end{cases}$$

Now, one can express the sum $\sigma_1(a)$ by means of $\sigma_0(a)$. For that, we compute in two ways the sum $\sum_{b\in\mathbb{F}_4^\star} S(a,b)$, for every $a \in \mathbb{F}_{2^m}^\star$.

Firstly,

$$\begin{aligned}\sum_{b\in\mathbb{F}_4^\star} S(a,b) &= \sum_{b\in\mathbb{F}_4^\star}\left(\sum_{j=0}^{2}\chi\left(\mathrm{Tr}_1^2(b\zeta^{\frac{j}{r}\frac{2^m+1}{3}})\right)\sigma_j(a)\right) \\ &= \sum_{j=0}^{2}\left(\sum_{b\in\mathbb{F}_4}\chi\left(\mathrm{Tr}_1^2(b\zeta^{\frac{j}{r}\frac{2^m+1}{3}})\right) - 1\right)\sigma_j(a).\end{aligned}$$

We get (since $\sigma_2(a) = \sigma_1(a)$)

$$\sum_{b\in\mathbb{F}_4^\star} S(a,b) = -\sum_{j=0}^{2}\sigma_j(a) = -\sigma_0(a) - 2\sigma_1(a).$$

Secondly, for $a \in \mathbb{F}_{2^m}^\star$, we have

$$\begin{aligned}\sum_{b\in\mathbb{F}_4^\star} S(a,b) &= \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au))\sum_{b\in\mathbb{F}_4^\star}\chi(\mathrm{Tr}_1^2(bu^{\frac{1}{r}\frac{2^m+1}{3}})) \\ &= \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au))\left(\sum_{b\in\mathbb{F}_4}\chi(\mathrm{Tr}_1^2(bu^{\frac{1}{r}\frac{2^m+1}{3}})) - 1\right).\end{aligned}$$

Hence,

$$\sum_{b\in\mathbb{F}_4^\star} S(a,b) = -\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au)).$$

Thanks to Proposition 2.3.1, we obtain

$$\sum_{b\in\mathbb{F}_4^\star} S(a,b) = K_m(a) - 1.$$

Collecting the two expressions of $\sum_{b\in\mathbb{F}_4^\star} S(a,b)$, we finally obtain:

$$\sigma_0(a) + 2\sigma_1(a) = 1 - K_m(a)$$

That is, $\sigma_1(a) = (1 - K_m(a) - \sigma_0(a))/2$.
Thus,

$$S(a,b) = \begin{cases} 2\sigma_0(a) + K_m(a) - 1 & \text{if } b = 1 \\ -\sigma_0(a) & \text{if } b \neq 1 \end{cases}$$

To conclude, we have to express the sum $\sigma_0(a)$ by means of Kloosterman sums and cubic sums. First, recall that, since n is even, the mapping $x \mapsto x^3$ is 3-to-1 from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Moreover, the mapping $x \mapsto x^3$ is also 3-to-1 from U to itself (since m is odd, 3 divides $2^m + 1$, the group $\mathbb{F}_4^\star$ is then contained in U). That implies in particular that

$$\sigma_0(a) := \sum_{v \in V} \chi(\mathrm{Tr}_1^n(av)) = \frac{1}{3} \sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^3)).$$

Thanks to the transitivity of trace function, we have $\mathrm{Tr}_1^n(au^3) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(au^3)) = \mathrm{Tr}_1^m(au^3 + (au^3)^{2^m})$. Then

$$\sigma_0(a) = \frac{1}{3} \sum_{u \in U} \chi(\mathrm{Tr}_1^m(a(u^3 + u^{-3}))).$$

Moreover, we make use of the fact, that every element $1/c$ where $c \in \mathbb{F}_{2^m}^\star$ with $\mathrm{Tr}_1^m(c) = 1$ can be uniquely represented as $u + u^{2^m}$ with $u \in U$. Note now that $1/c^3 + 1/c = u^3 + u^{-3}$. Therefore, using the fact that the mapping $c \mapsto 1/c$ is a permutation on $\mathbb{F}_{2^m}$, we obtain

$$\begin{aligned} \sigma_0(a) &= (1 + \sum_{u \in U \setminus \{1\}} \chi(\mathrm{Tr}_1^m(a(u^3 + u^{-3}))))/3 \\ &= (1 + 2 \sum_{\substack{c \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_1^m(c) = 1}} \chi(\mathrm{Tr}_1^m(a/c^3 + a/c)))/3 \\ &= (1 + 2 \sum_{\substack{c \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_1^m(1/c) = 1}} \chi(\mathrm{Tr}_1^m(ac^3 + ac)))/3 \end{aligned}$$

Now, Charpin et al. have proved in [57] that

$$2 \sum_{c \in \mathbb{F}_{2^m}, \mathrm{Tr}_1^m(1/c) = 1} \chi(\mathrm{Tr}_1^m(ac^3 + ac)) = 2C_m(a,a) - K_m(a)$$

from which we deduce that

$$\sigma_0(a) = (2C_m(a,a) + 1 - K_m(a))/3.$$

and then

$$S(a,b) = \begin{cases} (K_m(a) - 1 + 4C_m(a,a))/3 & \text{if } b = 1 \\ (K_m(a) - 1 - 2C_m(a,a))/3 & \text{if } b \neq 1 \end{cases}$$

□

In Chapter 5 and Chapter 8, we will need to produce necessary and suffisant conditions so that the sum involved in the previous proposition takes the value 1. To this end, we need the following statement.

Corollary 2.3.3. *([199]) Let $n = 2m$ with $m > 3$ odd. Let $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_4$ and r be a positive integer such that $\gcd(r, 2^m + 1) = 1$. Then*

$$\sum_{u \in U} \chi\left(\mathrm{Tr}_1^n(au^r) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right) = 1 \tag{2.1}$$

if and only if

- *$b = 0$ and $K_m(a) = 0$,*
- *or, $b \neq 0$ and $K_m(a) = 4$.*

Proof. Assume that (2.1) holds. Assume $b = 0$. According to Proposition 2.3.1, (2.1) is equivalent to $1 - K_m(a) = 1$, that is, $K_m(a) = 0$.
Assume $b \neq 0$. If $\mathrm{Tr}_1^m(a^{1/3}) = 0$ then $C_m(a, a) = 0$ according to Proposition 2.2.5. Thus, according to Proposition 2.3.2, (2.1) is reduced to $\frac{K_m(a)-1}{3} = 1$, that is, (2.1) is equivalent to $K_m(a) = 4$.
If $\mathrm{Tr}_1^m(a^{1/3}) = 1$. According to Proposition 2.2.5, $C_m(a, a) = C_m(1, a^{2/3}) = \epsilon_a \left(\frac{2}{m}\right) 2^{(m+1)/2}$ with $\epsilon_a = \pm 1$. Thus, according to Proposition 2.3.2, (2.1) is equivalent to $K_m(a) = 4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2}$ if $b \neq 1$ or $K_m(a) = 4 \pm \left(\frac{2}{m}\right) 2^{(m+5)/2}$ if $b = 1$. Now, Proposition 2.2.2 says that the Kloosterman sum $K_m(a)$ takes integer values in the range $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$. But, the values $4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2}$ and $4 \pm \left(\frac{2}{m}\right) 2^{(m+5)/2}$ do not belong to $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$ for every $m > 3$ proving that (2.1) is never satisfied if $\mathrm{Tr}_1^m(a^{1/3}) = 1$.
Conversely, assume that $b = 0$ and $K_m(a) = 0$. According to Proposition 2.3.1, $\sum_{u \in U} \chi(\mathrm{Tr}_1^n(au)) = 1 - K_m(a) = 1$. Assume that $b \neq 0$ and $K_m(a) = 4$. According to Proposition 2.2.3, $K_m(a) = 4$ implies that $\mathrm{Tr}_1^m(a^{1/3}) = 0$ and thus that $C_m(a, a) = 0$, thanks to Proposition 2.2.5. Equality (2.1) follows then from Proposition 2.3.2. □

The following technical result will also be useful in Chapter 8.

Proposition 2.3.4. *([199]) Let $n = 2m$ with m odd. Let $b \in \mathbb{F}_4^\star$, $a \in \mathbb{F}_{2^m}^\star$ and ζ be a generator of the cyclic group U. Let $i \in \{0, 1\}$. Then,*

If $m \not\equiv 3 \pmod 6$, we have

$$\sum_{u \in U} \chi\left(\mathrm{Tr}_1^n(a\zeta^i u^3) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right) = (K_m(a) - 1 + \mu_i C_m(a, a))/3.$$

where $\mu_0 = -2$ and $\mu_1 = 1$.

Proof. Set

$$S'(a, b) := \sum_{u \in U} \chi\left(\mathrm{Tr}_1^n(au^3) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right);$$

$$S''(a, b) := \sum_{u \in U} \chi\left(\mathrm{Tr}_1^n(a\zeta u^3) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right).$$

Keeping the same notation as in the proof of Proposition 2.3.2:
for $j \in \{0, 1, 2\}$, we set

$$\sigma_j(a) := \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^j v)).$$

Now, recall that m being odd, one can decompose U as follows

$$U = V \cup \zeta V \cup \zeta^2 V$$

where $V = \{u^3 \mid u \in U\}$. Thus, every element $u \in U$ can be uniquely decomposed as $u = \zeta^j v$ with $j \in \{0, 1, 2\}$ and $v \in V$.

Thus (in the second equality, we use the fact that the v is a cube of an element of U which is a cyclic group of order $2^m + 1$)

$$\begin{aligned} S'(a,b) &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^{3j} v^3) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}} v^{\frac{2^m+1}{3}})) \\ &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^{3j} v^3) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}})). \end{aligned}$$

Similarly,

$$\begin{aligned} S''(a,b) &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^{3j+1} v^3) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}} v^{\frac{2^m+1}{3}})) \\ &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^{3j+1} v^3) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}})). \end{aligned}$$

Now, since $m \not\equiv 3 \pmod 6$ then, integers 3 and $\frac{2^m+1}{3}$ are co-prime. The mapping $v \mapsto v^3$ is then a permutation of V and thus for $(i, j) \in \{0, 1, 2\}^2$, we have (in the second equality, we use the fact that the mapping $v \mapsto \zeta^{3j} v$ is a permutation of V)

$$\begin{aligned} S'(a,b) &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^{3j} v) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}})) \\ &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(av) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}})). \end{aligned}$$

Similarly,

$$\begin{aligned} S''(a,b) &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^{3j+1} v) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}})) \\ &= \sum_{j=0}^{2} \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta v) + \mathrm{Tr}_1^2(b\zeta^{j\frac{2^m+1}{3}})). \end{aligned}$$

Now, the set $\{b, b\zeta^{\frac{2^m+1}{3}}, b\zeta^{2\frac{2^m+1}{3}}\}$ is equal to $\mathbb{F}_4^\star$ (which contains two elements of absolute trace 1 on $\mathbb{F}_4$ and one element of absolute trace 0 on $\mathbb{F}_4$). We thus deduce that

$$\begin{aligned} S'(a,b) &= \sum_{v\in V}\chi(\mathrm{Tr}_1^n(av))\sum_{j=0}^{2}\chi(\mathrm{Tr}_1^2(b\zeta^j\tfrac{2^m+1}{3})) \\ &= -\sum_{v\in V}\chi(\mathrm{Tr}_1^n(av)) = -\sigma_0(a). \end{aligned}$$

Similarly,

$$\begin{aligned} S''(a,b) &= \sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\zeta v))\sum_{j=0}^{2}\chi(\mathrm{Tr}_1^2(b\zeta^j\tfrac{2^m+1}{3})) \\ &= -\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\zeta v)) = -\sigma_1(a). \end{aligned}$$

We thus conclude thanks to the relations between $\sigma_0(a)$, $\sigma_1(a)$, $K_m(a)$ and $C_m(a,a)$ (obtained in the proof of Proposition 2.3.2) that is,

$$\sigma_0(a) = (2C_m(a,a) + 1 - K_m(a))/3$$

and

$$\sigma_1(a) = (1 - K_m(a) - \sigma_0(a))/2.$$

□

In Chapter 8, we will need to exhibit necessary and suffisant conditions so that the sum involved in the previous proposition takes the value 1. To this end, we need the following statement.

Corollary 2.3.5. *([199]) Let $n = 2m$ with m odd. Let $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_4^\star$, ζ a generator of the cyclic group U and $i \in \{0,1\}$.*

a) If $m \not\equiv 3 \pmod 6$ then,

$$\sum_{u\in U}\chi\left(\mathrm{Tr}_1^n(a\zeta^i u^3) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right) = 1 \tag{2.2}$$

if and only if

- *$i = 0$ and $K_m(a) = 4$,*
- *or, $i = 1$ and $K_m(a) + C_m(a,a) = 4$.*

b) If $m \equiv 3 \pmod 6$ then

$$\sum_{u\in U}\chi\left(\mathrm{Tr}_1^n(a\zeta^i u^3) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right) \neq 1. \tag{2.3}$$

Proof.

a) Assume $m \not\equiv 3 \pmod 6$. Assume that (2.2) holds. If $i = 0$, equation (2.2) is equivalent to $K_m(a) = 4 + 2C_m(a,a)$ by Proposition 2.3.4. If $\mathrm{Tr}_1^m(a^{1/3}) = 0$ then, according to Proposition 2.2.5, $C_m(a,a) = 0$. Therefore, equation (2.2) is equivalent to $K_m(a) = 4$. If $\mathrm{Tr}_1^m(a^{1/3}) = 1$ then, according to Proposition 2.2.5, $C_m(a,a) = C_m(1,a^{2/3}) = \epsilon_a\left(\frac{2}{m}\right)2^{(m+1)/2}$ with $\epsilon_a = \pm 1$. But,

$4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2} \notin [-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$.
Now, if $i = 1$, equation (2.2) is equivalent to $K_m(a) + C_m(a,a) = 4$, by Proposition 2.3.4. Conversely, let us prove (2.2). Assume $i = 0$ and $K_m(a) = 4$. That implies that $\mathrm{Tr}_1^m(a^{1/3}) = 0$ (by Proposition 2.2.3) and thus that $C_m(a,a) = 0$ (by Proposition 2.2.5). Equation (2.2) follows then from the first identity of Proposition 2.3.4. Likewise, in the case where $i = 1$ and $K_m(a) + C_m(a,a) = 4$, equation (2.2) is deduced from the second identity of Proposition 2.3.4.
b) Assume $m \equiv 3 \pmod 6$. Then $2^m + 1$ is a multiple of 9. Therefore, the mapping $u \mapsto u^3$, being 3-to-1 from U to itself, we have

$$\sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(a\zeta^i u^3) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right) = 3\sum_{v\in V} \chi\left(\mathrm{Tr}_1^n(a\zeta^i v) + \mathrm{Tr}_1^2(bv^{\frac{2^m+1}{9}})\right)$$

where $V = \{u^3,\, u \in U\}$, which implies (2.3). □

Finally, we also have to express another type of exponential sums over U in terms of Kloosterman sums and cubic sums. This result will be useful in Chapter 5.

Proposition 2.3.6. *([199]) Let m be an odd integer. Let $a \in \mathbb{F}_{2^m}^\star$. U denotes the set of the (2^m+1)-th roots of unity in $\mathbb{F}_{2^n}$. Then, we have*

$$\sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^3)) = 1 - K_m(a) + 2C_m(a,a).$$

Proof. Using the transitivity rule of trace function, we have

$$\mathrm{Tr}_1^n(au^3) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(au^3)) = \mathrm{Tr}_1^m(au^3 + (au^3)^{2^m}).$$

Hence

$$\sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^3)) = \sum_{u\in U} \chi(\mathrm{Tr}_1^m(a(u^3+u^{-3}))).$$

Now, recall that every element $1/c$ where $c \in \mathbb{F}_{2^m}^\star$ with $\mathrm{Tr}_1^m(c) = 1$ can be uniquely represented as $u + u^{2^m}$ with $u \in U$. Therefore, since $1/c^3 + 1/c = u^3 + u^{-3}$ (indeed, $1/c^3 = (u+u^{2^m})^3 = (u+u^{-1})^3 = u^3 + u^{-3} + uu^{-1}(u+u^{-1}) = u^3 + u^{-3} + 1/c$) , we have

$$\begin{aligned}
\sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^3)) &= 1 + \sum_{u\in U\setminus\{1\}} \chi(\mathrm{Tr}_1^m(a(u^3+u^{-3}))) \\
&= 1 + 2\sum_{\substack{c\in\mathbb{F}_{2^m} \\ \mathrm{Tr}_1^m(c)=1}} \chi(\mathrm{Tr}_1^m(a/c^3 + a/c)) \\
&= 1 + 2\sum_{\substack{c\in\mathbb{F}_{2^m} \\ \mathrm{Tr}_1^m(1/c)=1}} \chi(\mathrm{Tr}_1^m(ac^3 + ac))
\end{aligned}$$

In the last equality, we use the fact that the map $c \mapsto 1/c$ is a permutation on $\mathbb{F}_{2^m}$. Now, Charpin, Helleseth and Zinoviev have proved in [57] that when m is odd, we have

$$2\sum_{c\in\mathbb{F}_{2^m}, \mathrm{Tr}_1^m(1/c)=1} \chi(\mathrm{Tr}_1^m(ac^3+ac)) = 2C_m(a,a) - K_m(a).$$

from which we deduce the result. □

2.4 Binary Dickson polynomial

The family of binary *Dickson polynomials* $D_r(X) \in \mathbb{F}_2[X]$ of degree r is defined by

$$D_r(X) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \frac{r}{r-i} \binom{r-i}{i} X^{r-2i}, \quad r = 2, 3, \cdots$$

Dickson polynomials can also be defined by the following recurrence relation:

$$D_{i+2}(X) = XD_{i+1}(X) + D_i(X)$$

with initial values

$$D_0(X) = 0, \quad D_1(X) = X.$$

For any non-zero positive integers r and p, Dickson polynomials satisfy:

1. $\deg(D_r(X)) = r$,
2. $D_{rp}(X) = D_r(D_p(X))$,
3. $D_r(x + x^{-1}) = x^r + x^{-r}$.

The reader can refer to [224] for many useful properties and applications of Dickson polynomials. We give the list of the first eleven Dickson polynomials:
$D_0(X) = 0$
$D_1(X) = X$
$D_2(X) = X^2$
$D_3(X) = X + X^3$
$D_4(X) = X^4$
$D_5(X) = X + X^3 + X^5$
$D_6(X) = X^2 + X^6$
$D_7(X) = X + X^5 + X^7$
$D_8(X) = X^8$
$D_9(X) = X + X^5 + X^7 + X^9$
$D_{10}(X) = X^2 + X^6 + X^{10}$

Dillon and Dobbertin [88, pp 355–356] remarked that a more careful analysis shows that Dickson polynomials leave the sets of elements whose inverses have a given absolute trace fixed. [2]

Lemma 2.4.1 ([88], [102, Lemma 1]). *Let $r \geq 0$ be an integer and $x \in \mathbb{F}_{2^m}$. Then*

$$\mathrm{Tr}_1^m\left(\frac{1}{D_r(x)}\right) = \mathrm{Tr}_1^m\left(\frac{1}{x}\right) \ .$$

This property was recently used and reproved in a elementary way by Charpin, Helleseth and Zinoviev [61, Proof of Lemma 14] for D_3, as well as Wang et al. [257, Proof of Proposition 5] for the case D_5, who remarked that

$$\frac{1}{D_3(x)} = \frac{1}{x} + \frac{1}{x+1} + \frac{1}{x^2+1}, \ \frac{1}{D_5(x)} = \frac{1}{x} + \frac{x}{x^2+x+1} + \frac{x}{x^4+x^2+1} \ .$$

A much more general fact is actually true as we now demonstrate in an alternative manner. To this end auxiliary polynomials are needed.

[2] A weaker statement is also proved by Ranto [225, Lemma 4] who assumes that $k = \gcd(r, 2^m - 1) = 1$.

Definition 2.4.2. *Let $r \geq 0$ be an integer. Define the polynomial $f_r(x)$ as*

$$D_r(x) = \begin{cases} xf_r(x)^2 & \text{if } r \text{ is odd} \ , \\ x^2 f_r(x)^2 & \text{if } r \text{ is even} \ . \end{cases}$$

The following relation between D_r and f_r is then verified.

Lemma 2.4.3. *([102]) Let $r \geq 0$ be an integer. Then*

$$x + D_r(x) + x^2 f_r(x) f_{r+1}(x) + D_{r+1}(x) = 0 \ .$$

Proof. We equivalently show that

$$x^2 + D_r(x)^2 + x^4 f_r(x)^2 f_{r+1}(x)^2 + D_{r+1}(x)^2 = 0 \ ,$$

which can be rewritten as

$$x^2 + D_r(x)^2 + xD_r(x)D_{r+1}(x) + D_{r+1}(x)^2 = 0 \ .$$

For $r = 0$, this is trivially verified. For $r \geq 1$, write down $D_{r+1}(x)$ as $D_{r+1}(x) = xD_r(x) + D_{r-1}(x)$ and the result follows by induction. □

As a corollary we get a general expression for $\frac{1}{D_r(x)}$ involving $f_r(x)$.

Corollary 2.4.4. *([102]) Let $r \geq 1$ be an integer. Then*

$$\begin{aligned} \frac{1}{D_r(x)} &= \frac{1}{x} + \frac{f_{r-1}(x)}{f_r(x)} + \frac{f_{r-1}(x)^2}{f_r(x)^2} \ , \\ &= \frac{1}{x} + \frac{f_{r+1}(x)}{f_r(x)} + \frac{f_{r+1}(x)^2}{f_r(x)^2} \ . \end{aligned}$$

Proof. Since $D_{2r}(x) = D_r(x)$, we can assume that r is odd without loss of generality. Then

$$\begin{aligned} \frac{1}{D_r(x)} &= \frac{1}{xf_r(x)^2} = \frac{x}{x^2 f_r(x)^2} \\ &= \frac{D_r(x) + x^2 f_r(x) f_{r+1}(x) + D_{r+1}(x)}{x^2 f_r(x)^2} \\ &= \frac{xf_r(x)^2 + x^2 f_r(x) f_{r+1}(x) + x^2 f_{r+1}(x)^2}{x^2 f_r(x)^2} \\ &= \frac{1}{x} + \frac{f_{r+1}(x)}{f_r(x)} + \frac{f_{r+1}(x)^2}{f_r(x)^2} \ ; \end{aligned}$$

the other equality being deduced in a similar way. □

Lemma 2.4.1 directly follows from Corollary 2.4.4, thus yielding an alternative and more concrete proof of it.

A well-known result by Chou, Gomez-Calderon and Mullen [66] describes the cardinality of the preimage of an arbitrary element.

Theorem 2.4.5 ([66, Theorem 9], [167, Theorem 3.26])**.** *Let $\mathbb{F}_{2^m}$ be the finite field with 2^m elements and $1 \leq r \leq 2^n - 1$ be an integer. Let*

$$k = \gcd(r, 2^m - 1), \ \ l = \gcd(r, 2^m + 1) \ .$$

Let $x, y \in \mathbb{F}_{2^m}$ be two elements such that $D_r(x) = y$. Then

$$\#D_r^{-1}(y) = \begin{cases} \frac{k+l}{2} & \text{if } y = 0 \ , \\ k & \text{if } y \neq 0 \text{ and } \mathrm{Tr}_1^m(1/x) = 0 \ , \\ l & \text{if } y \neq 0 \text{ and } \mathrm{Tr}_1^m(1/x) = 1 \ . \end{cases}$$

As a corollary, they obtain the cardinalities of the value sets of Dickson polynomials [66, Theorems 10 and 10'], [167, Theorems 3.27 and 3.30], and in particular a proof of the characterizations of Dickson polynomials as permutation polynomials [66, Corollary 11], [167, Corollary 3.28].

The proof heavily relies on the study of the map

$$\begin{aligned} \mathbb{F}_{2^n} &\to \mathbb{F}_{2^m} \\ x &\mapsto x + x^{-1} \end{aligned}$$

and Waring's formula [167, Theorem 1.1], [168, Theorem 1.76] which ensures that [167, Equation 2.2], [168, Equation 7.8]

$$D_r(x + x^{-1}) = x^r + x^{-r} \ .$$

The following property is then a corollary to the above results.

Corollary 2.4.6. *([102]) Let $1 \leq r \leq 2^n - 1$ be an integer. Then the map $x \mapsto D_r(x)$ induces a permutation of*

- *$\mathcal{T}_0$ if and only if $k = \gcd(r, 2^m - 1) = 1$;*
- *$\mathcal{T}_1$ if and only if $l = \gcd(r, 2^m + 1) = 1$.*

Proof. Lemma 2.4.1 shows that D_r maps $\mathcal{T}_i$ into $\mathcal{T}_i$ for $i \in \mathbb{F}_2$. One then concludes using Theorem 2.4.5 which gives the size of the preimage of $x \in \mathcal{T}_i$. □

We define the corresponding exponential sums as follows. Recall that for a Boolean function $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$, its *"sign" function* is the integer-valued function $\chi(f) = \chi_f = (-1)^f$, i.e. f composed with the additive character of $\mathbb{F}_2$.

Definition 2.4.7. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. We denote by $T_i^r(f)$ the exponential sum on $\mathcal{T}_i$ for $i \in \mathbb{F}_2$ for $f \circ D_r$, that is*

$$T_i^r(f) = \sum_{x \in \mathcal{T}_i} \chi_{f \circ D_r}(x) \ .$$

Moreover, let $T_i(f) = T_i^1(f)$.

The following lemma is easily deduced from the equality $(-1)^{\mathrm{Tr}_1^m(x)} = 1 - 2\,\mathrm{Tr}_1^m(x)$ where the values of the trace are understood as the integers 0 and 1.

Lemma 2.4.8. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Then*

$$T_i(f) = \frac{1}{2}\left(\sum_{x \in \mathbb{F}_{2^m}} \chi_f(x) + (-1)^i \sum_{x \in \mathbb{F}_{2^m}} \chi\left(\mathrm{Tr}_1^m(1/x) + f(x)\right) \right) \ .$$

And we finally record the following corollary.

Corollary 2.4.9. *Let $1 \leq r \leq 2^n - 1$ be an integer and $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function. Assume moreover that $\gcd(r, 2^m - 1) = 1$. Then*

$$\begin{aligned} T_0^r(f) &= T_0(f) \ , \\ T_1^r(f) &= \sum_{x \in \mathbb{F}_{2^m}} \chi_{f \circ D_r}(x) - T_0(f) \ . \end{aligned}$$

Chapter 3

Boolean functions and cryptography

Contents

3.1 Cryptographic framework for Boolean functions

Stream ciphers are commonly used for encrypting and decrypting messages. Stream ciphers have several advantages which make them suitable for some applications. Most notably, they are usually faster and have a lower hardware complexity than block ciphers. They are for instance appropriate when buffering is limited, since the binary digits are individually encrypted and decrypted. In stream cipher the encryption and the decryption consists in adding bitwise the input stream and a pseudo random sequence generated by a pseudo-random generator taking as input a secret information, the secret key. Classical tools to produce such pseudo-random sequences, that are called keystream, are Linear Feedback Registers (LFSR). Stream ciphers can use several LFSR or a single LFSR. As indicated by its name, LFSR are linear and linear systems are governed by linear relationships between their inputs and outputs. Since linear dependencies can relatively easily be analyzed, stream ciphers designed only with LFSR would be highly insecure.

To produce more secure encryption scheme, Boolean functions are used to produce the keystream from LSFR entries. Stream ciphers often use a single Boolean to have a good efficiency, that is, to be extremely fast in hardware and software. The Boolean function allows to make the relationship between the plaintext and the ciphertext as complex as possible. More precisely, a bit of the ciphertext is obtained from a bit of the plaintext by adding bitwise a key digit (the ouput of the Boolean function) whose dependance upon the LFSR entries (the secret information) is nonlinear. Thus, the security of such cryptosystems deeply relies on the choice of the Boolean function because the complexity of the relationship between the plaintext and the ciphertext depends entirely on the Boolean function. Indeed, some properties of the Boolean function can be exploited to gain access to the contents of encrypted messages, even if the key is unknown. Therefore Boolean functions needs to have some important characteristics to resist to several types of attacks that are called security criteria.

Classical models for such cryptosystems are stream ciphers: this design is loosely based on the one-time pad [191, 6.1.1], or Vernam cipher, for which a random keystream is used to encrypt the plaintext one bit at a time. Hence, to build a stream cipher, a suitable pseudorandom keystream generator must be designed. A common construction is to use one or several linear feedback shift registers [191, 6.2.1] (LFSR) filtered or combined by a Boolean function. The filtered model is usually composed of one or several LFSR's, and of a nonlinear combining or filtering function f which produces the output, given the state of the linear part. In the combiner generator model, the outputs to several Linear Feedback Shift Registers are combined by a Boolean function giving, at each clock cycle, one bit of the pseudo-random sequence. Both models are depicted in Figures 3.1 and 3.2.

3.2 Main cryptographic criteria for Boolean functions

The design of conventional cryptographic systems relies on two fundamental principles introduced by Claude Shannon in his paper [233] Communication Theory of Secrecy Systems, published in 1949. : *confusion* and *diffusion* . In cryptography, confusion and diffusion are two properties of the operation of a secure cipher. Confusion aims at concealing any algebraic structure in the system. It is closely related to the complexity (that is, the cryptographic complexity, which is different from circuit complexity, for instance.) of the involved Boolean functions. In Shannon's original definitions, confusion refers to making the relationship between the plaintext and the ciphertext as complex and involved as possible; diffusion refers to the property that the redundancy in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext. In other words, the

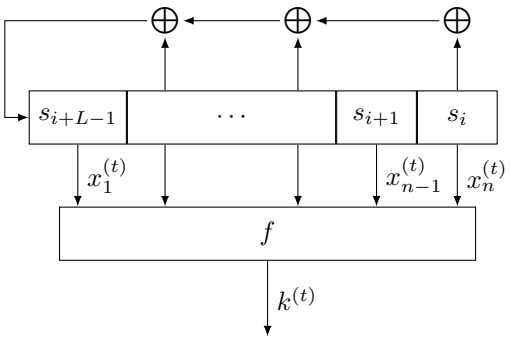

Figure 3.1 – The filter model

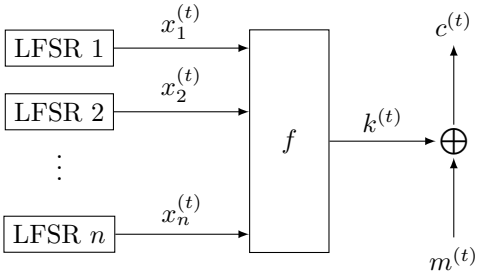

Figure 3.2 – The combiner model

non-uniformity in the distribution of the individual letters (and pairs of neighbouring letters) in the plaintext should be redistributed into the non-uniformity in the distribution of much larger structures of the ciphertext, which is much harder to detect. Diffusion means that the output bits should depend on the input bits in a very complex way. In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable or pseudorandom manner. Diffusion consists then in spreading out the influence of any minor modification of the input data or of the key over all outputs.

These two principles were stated more than half a century ago. Since then, many attacks have been found against the diverse known cryptosystems, and the relevance of these two principles has always been confirmed. The known attacks on each cryptosystem lead to criteria that the implemented cryptographic functions must satisfy. More precisely, the resistance of the cryptosystems to the known attacks can be quantified through some fundamental characteristics (some, more related to confusion, and some, more related to diffusion) of the Boolean functions used in them; and the design of these cryptographic functions needs to consider various characteristics simultaneously.

3.2.1 The algebraic degree

The linear complexity of the pseudorandom generator depends on the algebraic degree of its filtering or combining function, whence the importance for it to have a high algebraic degree in order to avoid the Berlekamp–Massey attacks [180], [191, 6.2.3], [31, 4.1.1] and, for the filter model, the more recent Rønjom–Helleseth attack [226]. It is obviously verified from the definition

of the algebraic normal form that the algebraic degree of a Boolean function in n variables is at most n.

3.2.2 Balancedness

To avoid statistical dependence between the input (the plaintext) and the output (the ciphertext.) of the stream cipher and to prevent distinguishing attacks [31, 4.1.3], cryptographic functions must be *balanced* functions. A balanced Boolean function is a function whose output yields as many 0s as 1s over its input set. This means that for a uniformly random input string of bits, the probalility of getting a 1 is $\frac{1}{2}$. Equivalently, a Boolean function in n variables is said to be balanced if it has Hamming weight 2^{n-1}. Note that the algebraic degree of an n-variable Boolean function is at most $n-1$.

3.2.3 The nonlinearity

The cryptographic criterion of interest in this manuscript (in particular in Chapter 4) is that of nonlinearity and the related notion of bentness. Nonlinearity characterizes the distance between a Boolean function and the set of affine functions (i.e. those of algebraic degree 0 or 1) and is naturally defined using the Hamming distance. More precisely, the nonlinearity of f, denoted by $nl(f)$, is the minimum distance to affine functions (in terms of Reed-Muller codes, it is equal to the minimum distance of the linear code Reed-Muller code $\mathcal{RM}(1,n) \cup (f + \mathcal{RM}(1,n))$ where $\mathcal{RM}(1,n)$ denote the Reed-Muller code of order 1 and length 2^n). It can be shown that the nonlinearity of a Boolean function in n variables is upper bounded by $2^{n-1} - 2^{n/2-1}$. In order to provide confusion, cryptographic functions must lie at large Hamming distance (in the sens, close to the maximum value $2^{n-1} - 2^{n/2-1}$) to all affine functions, equivalently must be of a large nonlinearity (in the sens, close to the upper bound $2^{n-1} - 2^{n/2-1}$). Boolean functions achieving maximal nonlinearity are called bent functions but such functions can not be directly used in the filter and combiner models; in particular, they are not balanced.

Nonlinearity criteria for Boolean functions are classified in view of their suitability for cryptographic design. The classification is set up in terms of the largest transformation group leaving a criterion invariant. In this respect two criteria turn out to be of special interest, the distance to linear structures and the distance to affine functions, which are shown to be invariant under all affine transformations. A high nonlinearity is surely one of the most important cryptographic criteria. In the case of stream ciphers, high nonlinearity is important to prevent fast correlation attacks [190] and best affine approximation attacks [89]. The larger is the nonlinearity, the less efficient are fast correlation attacks [22, 64, 107, 141, 140, 142, 188] and linear attack[1].

3.2.4 Correlation immune and resiliency

To avoid a divide and conquer attack, called *correlation attack* (see *e.g.*[22, 251, 187, 237]) on the combiner model, the combining function must avoid low order correlation . This is the reason why such a combining function is often chosen with a rather high correlation immunity order. There are two equivalent ways for characterising the correlation immunity: either by means of the Walsh transform or by means of the sub-functions. Originally, an n-variable Boolean function f is said to be *correlation immune* of order t (or t-th order correlation immune) if any sub-function deduced from f by fixing at most t inputs has the same output distribution as f. On the other hand,

[1]We shall say that there is a correlation between a Boolean function f and a linear function ℓ if $d_H(f,\ell)$ is different from 2^{n-1}. Any Boolean function has correlation with some linear functions of its input. But this correlation should be small: the existence of affine approximations of the Boolean functions involved in a cryptosystem allows in various situations (block ciphers, stream ciphers) to build attacks on this system ([267, 182]).

correlation immunity can be characterised by means of the Walsh transform of f. A Boolean function f is said correlation immune of order t if and only if the Walsh transform of f vanishes at all non zero vector of Hamming weight at most t ([266]). If f is moreover balanced, then f is said to be t-resilient. This definition of resiliency was introduced by Siegenthaler in [236]. If f is not m-resilient, then there exists a correlation between the output to the function and (at most) m coordinates of its input; if m is small, the divide-and-conquer attack uses this weakness for attacking a system using f as combining function. To conclude, briefly, a Boolean function used in the combiner model should be resilient in order to resist correlation attacks [237]. This is not mandatory for functions used in the filter model. In the latter model, 1-resiliency is commonly considered to be sufficient and can be obtained by choosing another function in the same affine equivalence class.

3.2.5 Algebraic immunity

Standard algebraic attacks were introduced in 2003 by Courtois and Meier [75]. Algebraic attacks recover the secret key, or at least the initialization of the system, by solving a system of multivariate algebraic equations. The idea that the key bits can be characterized as the solutions of a system of multivariate equations comes from C. Shannon [233]. In practice, for cryptosystems which are robust against the usual attacks such as the Berlekamp-Massey attack, this system is too complex to be solved [2](its equations being highly nonlinear). However, in the case of stream ciphers, we can get a very overdefined system (i.e. a system with a number of linearly independent equations much greater than the number of unknowns). In view of these attacks, the study of the set of annihilators of a Boolean function has become very important and a Boolean function should have a high *algebraic immunity*. We define these notions below.

Definition 3.2.1 (Annihilator [189])**.** *Let f be a Boolean function in n variables. A nonzero Boolean function g is called an annihilator of f if $fg = 0$.*

Definition 3.2.2 (Algebraic immunity [189])**.** *The algebraic immunity of f, denoted by $AI(f)$, is the minimum value of d such that f or its complement $1 + f$ admits an annihilator of algebraic degree d.*

Clearly, the algebraic immunity of a Boolean function f is less than or equal to its algebraic degree since $1 \oplus f$ is an annihilator of f. As shown in [75], the algebraic immunity of any n-variable function is bounded by $\lceil n/2 \rceil$. Moreover, it was shown in [77] that the Hamming weight of a Boolean function f with given algebraic immunity satisfies : $\sum_{i=0}^{AI(f)-1} \binom{n}{i} \leq \mathrm{wt}(f) \leq \sum_{i=0}^{n-AI(f)} \binom{n}{i}$. In particular, if n is odd and f has optimum algebraic immunity then f is balanced.

A high value of algebraic immunity is now an absolutely necessary cryptographic criterion for a resistance to algebraic attacks but is not sufficient, because of a more general kind of attacks was indeed introduced by Courtois [74] in 2003 as well, called *fast algebraic attacks*[3] (which work if one can find g of low degree and $h \neq 0$ of reasonable degree such that $fg = h$, see [74, 122]).

[2]The number of equations can then be much larger than the number of unknowns. This makes less complex the resolution of the system by using Groebner basis (see [99]), and even allows linearizing the system (i.e. obtaining a system of linear equations by replacing every monomial of degree greater than 1 by a new unknown); the resulting linear system has however too many unkwnowns and cannot be solved.

[3]For these attacks, the product of f or its complement $1 + f$ with another function g of low degree should not be zero, as for standard algebraic attacks, but of lower degree, hence generalizing the former attacks and making the notion of algebraic immunity already insufficient.

3.3 Trade-offs between the different criteria

Cryptographic functions having the maximum nonlinearity (that is, bent functions) are never balanced. Moreover, Siegenthaler's bound [236] states that the algebraic degree of an n-variable t-th order correlation immune Boolean function is necessarily less than or equal to $n-t$ [236]. On the other hand, the nonlinearity of a t-th order correlation immune Boolean function is necessarily less than or equal to $2^{n-1}-2^t$ if $t > \frac{n}{2}-1$ and $2^{n-1}-2^{\frac{n}{2}-1}-2^t$ otherwise [46]. When the Boolean function is moreover balanced, the upper bounds on its algebraic degree and its nonlinearity are lower. Indeed, the algebraic degree is less than or equal to $n-t-1$ and the nonlinearity is upper bounded by $2^{n-1}-2^{t+1}$ if $\frac{n}{2}-1 < t < n-1$ and $2^{n-1}-2^{\frac{n}{2}-1}-2^{t+1}$ if $t \leq \frac{n}{2}-1$. Therefore, the correlation immunity criterion is not compatible with a high algebraic degree (necessary to withstand Berlekamp-Massey attack) and a high nonlinearity (necessary for avoiding attacks using linear approximation of the function). Moreover, the recent algebraic attacks, *e.g* [72, 73], highlighted the need for having a high algebraic degree as well as a high algebraic immunity so that stream ciphers can resist to these attacks. Now, there seems to be some kind of contradiction for Boolean functions between having high correlation immunity and optimum or nearly optimum algebraic immunity; also, much attention having been given to algebraic immunity recently, several examples of functions having optimum algebraic immunity could be found but no example of correlation immune Boolean function with optimum algebraic immunity.

As we have seen, there are numerous cryptographic requirements for Boolean functions (in fact there exist other criteria such as Strict Avalanche criterion and propagation criterion (see [31], Section 8.4.1, pages 303-305 and pages 308-311). Cryptographic function must necessarily satisfy some of them bearing on balancedness, algebraic degree, nonlinearity, algebraic immunity and must have a good resistance to fast algebraic attacks. Such properties allow the system designer to quantify the level of resistance of the system to attacks. It is often impossible to satisfy simultaneously several criteria at once, so that compromises have to be made, and trade-offs need to be quantified . Indeed, the difficulty precisely lies in finding the best trade-offs between all criteria and proposing concrete constructions of functions achieving them. An additional important motive is the fact that the current situation of symmetric cryptography is rather fragile because of recent progress in cryptanalysis. As explained Claude Carlet in his Book's Chapter dealing with Boolean functions ([31]), it is difficult but not impossible to find functions satisfying good trade-offs between all these criteria. It is not clear whether it is possible to achieve additionally resiliency of a sufficient order[4], which is necessary for the combiner model. Hence, the filter model may be more appropriate (future research will determine this).

3.4 Relaxing a cryptographic criterion: the concept of immunity profile

As observed in [155], strict correlation immunity is not absolutely required. The work factor to reconstitute the sequences coming from several registers increases with the number of registers, and a strict correlation immunity is necessary for small orders only. For higher orders, low non-zero correlations are sufficient (the lower the order, the lower the allowed correlations). In [155], the authors allow the restrictions to have output distributions slightly differing from the distribution of the global function. We propose here an alternate way of relaxing the constraint of correlation immunity. We allow the Walsh transform to take low values for low orders instead of being null. We introduce the concept of *immunity profile* of a Boolean function.

[4]First-order resiliency is useful for resisting some distinguishing (less dreadful) attacks.

3.4.1 φ-Correlation Immune Boolean functions

Definition 3.4.1. *([40]) Let n be any integer, $n \geq 2$. Let φ be any integer valued mapping over the set $\{0, \ldots, n\}$. A Boolean function f over $\mathbb{F}_2^n$ is said to be φ-correlation immune if, for any vector $\omega \in \mathbb{F}_2^n$,*

$$|\widehat{\chi_f}(\omega)| \leq \varphi(\mathrm{wt}(\omega))$$

where $\mathrm{wt}(\omega)$ denotes the Hamming weight of vector ω. If f is moreover balanced then f is said to be φ-resilient. The integer mapping φ is called the immunity profile *of f.*

This definition generalizes correlation immunity as t-th order correlation immune Boolean functions are φ-correlation immune with $\varphi(i) = 0$ for $1 \leq i \leq t$ and $\varphi(i) = 2^n$ for $i \geq t+1$ or $i = 0$. Every Boolean function is clearly φ-correlation immune for some φ. It is advisable to carefully choose the integer mapping φ. It seems natural to consider increasing mappings φ, which take low values for low orders.

Remark 3.4.2. *Let f be a φ-correlation immune Boolean function for some integer valued mapping φ over $\{0, \ldots, n\}$. Because of Parseval's identity that states that $\sum_{\omega \in \mathbb{F}_2^n} \widehat{\chi_f}^2(\omega) = 2^n$, the immunity profile φ of f must satisfy*

$$\sum_{l=0}^{n} \binom{n}{l} \varphi^2(l) \geq 2^{2n}. \tag{3.1}$$

Remark 3.4.3. *The constraint on the algebraic degree stated by Siegenthaler's bound can be avoided for φ-correlation immune Boolean function if φ is carefully chosen.*

3.4.2 Which immunity profile ?

Fast correlation attacks

Consider a stream generator constituted of n LFSR's. Each of them is of dimension about k and they are combined by an n-variable Boolean function f.

The adversary observes a sample of N bits of the keystream and must recover the initial state of each register. He may have several strategies. He can try to get initial state of a single LFSR, of two at once, or more.

Fast correlation attacks model the nonlinear function (in all models) as a noise on a communication channel with error probability $p = \frac{1}{2} - \varepsilon$, and the cryptanalysis as a decoding problem of length N, the amount of available keystream, and of dimension at most $k\ell$, where ℓ denotes the number of registers the adversary decides to recover by this decoding process [22, 251, 187, 203, 206]. More precisely, the nonlinear function is modelled by a Binary Symmetric Channel with transition probability p given by

$$p = \frac{1}{2} - \varepsilon \text{ with } \varepsilon = \frac{\varphi(\ell)}{2^{n+1}} \text{ and } \varphi(\ell) = \max_{u, \mathrm{wt}(u)=\ell} |\widehat{\chi_f}(u)|, \tag{3.2}$$

that corresponds to the maximum correlation between the output to f and the combination of ℓ LFSR states, by means of some ℓ-variable Boolean function, that the adversary decides to recover. When f is ℓ-th order correlation immune (this corresponds to the case where $p = \frac{1}{2}$), the adversary has no chance to recover the internal state of ℓ registers while if f is not ℓ-resilient the cryptanalyst can theoretically recover the state of the registers. Obviously, from a practical viewpoint, the success of the cryptanalyst will not be guaranteed either if he does not know enough keystream bits or if the complexity of the decoding procedure is too high. We will consider

separately each of the two situations. This will lead us to different immunity profiles for the Boolean function combining the LFSR's (indeed, the limitation factor can come from the data or from the computation power).

From an information theory point of view, the data at the disposal of the adversary must be sufficient to recover the initial state of the registers and the error vector, thus, the size N of the sample must satisfy the following inequality (Shannon's channel coding theorem, see *e.g.* [174]):

$$N \geq \frac{k\ell}{1-h_2(p)}, \tag{3.3}$$

where $h_2 : p \mapsto -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function. Whenever ε is small, one has $1 - h_2(p) \approx \frac{2}{\ln(2)}\left(p - \frac{1}{2}\right)^2$. Thus, the condition (3.3) of success for the adversary becomes $k\ell \leq \frac{2N}{\ln(2)}\frac{\varphi(\ell)^2}{2^{2n+2}}$. Consequently, if the resiliency profile φ satisfies at ℓ

$$\varphi(\ell) \leq 2^n \sqrt{\frac{2k\ln(2)}{N}} \cdot \sqrt{\ell} \tag{3.4}$$

then, the adversary has no chance to decode if he has only N bits of the keystream. In conclusion, get an ℓ-resilient nonlinear function may not be the best choice as this implies, among other drawbacks, that this function has higher correlations of order $\geq \ell + 1$. Such a function may allow the adversary to apply with greater success a decoding strategy to $\ell + 1$ LFSR at once. Choosing a function with a resiliency profile that increases in proportion to the square root of the order ℓ makes the resistance to correlation attack more homogeneous. We stress that this immunity profile is defined from the point of view of information theory independently from the complexity of the decoding procedure. Because of (3.1), there could exist Boolean functions whose immunity profile satisfies inequality (3.4) only if, for fixed N and k, n satisfies $n2^n \geq \frac{N}{k\ln(2)}$.

An alternative approach is to define the immunity profile according to the complexity of the decoding procedures. Mainly two different approaches have been proposed in the literature. The first approach [251] consists in associating a smaller linear code of dimension $\alpha k\ell$ (with $\alpha < 1$) to the keystream on which a maximum-likelihood procedure is performed. The resulting complexity of the decoding step is about $\mathcal{O}\big(\varepsilon^{-2t} \cdot 2^{\alpha k\ell} \cdot k\alpha\ell\big)$ (where t is some positive integer). The second approach [22] uses the existence of low-density parity-check equations to perform an efficient iterative decoding algorithm. When parity-check equations with weight w are used, the complexity of their decoding procedure is about $\mathcal{O}\Big(\big(\frac{1}{\varepsilon}\big)^{\frac{2w(w-2)}{w-1}} 2^{\frac{k\ell}{w-1}}\Big)$. Consequently, if the immunity profile φ is such that $\varphi(\ell) \leq 2^{\beta\ell}$ for $\ell > 0$ then the complexity of the decoding procedure of the first approach [251] would be greater than $\mathcal{O}\Big(2^{2t(n+1)} \cdot 2^{(\alpha k - 2t\beta)\ell} \cdot \alpha k\ell\Big)$ while the complexity of the second approach [22] would be greater than $\mathcal{O}\Big(2^{\frac{2w(w-2)}{w-1}(n+1)} \cdot 2^{\frac{k-2w(w-2)\beta}{w-1}\ell}\Big)$. Basically, decoding the keystream of a combiner generator could be a very hard problem even if the LFSR registers are combined through a Boolean function f with an exponential immunity profile, that is, of the form $\varphi(\ell) = \lambda 2^{\beta\ell}$, $\ell \neq 0$ (the lower the values of β and λ, the more secure the stream cipher).

Composition of Boolean functions

Let k be an integer greater than or equal to 2 and consider a Boolean function f over $\mathbb{F}_2^k$. For each $i \in \{1, \ldots, k\}$, let n_i be an integer greater than or equal to 2 and f_i be a Boolean function over $\mathbb{F}_2^{n_i}$. The composition of f by the f_i's is by definition the Boolean function F over $\mathbb{F}_2^{n_1} \times \cdots \times \mathbb{F}_2^{n_k}$ defined by $(x_1, \ldots, x_k) \mapsto f\big(f_1(x_1), \ldots, f_k(x_k)\big)$. Such a construction appears in iterated ciphers where a high complexity ciphering function is required, for example in a self

synchronizing stream cipher. In a block cipher, vector valued functions are used, but the analysis principle is quite similar. In order to apply a linear cryptanalysis, a linear approximation of the ciphering function is required and the best approximation is given by the analysis of the above construction. On the other hand, the designer must take care at constructing highly nonlinear ciphering function. By definition, the Walsh transform of the iterated function F is, for any vector $(u_1, \ldots, u_k) \in \mathbb{F}_2^{n_1} \times \cdots \times \mathbb{F}_2^{n_k}$,

$$\widehat{\chi_F}(u_1, \ldots, u_k) = \sum_{(x_1,\ldots,x_k)\in\mathbb{F}_2^{n_1}\times\cdots\times F_2^{n_k}} (-1)^{f\left(f_1(x_1),\ldots,f_k(x_k)\right)+u_1\cdot x_1+\cdots+u_k\cdot x_k}$$

This expression can be expressed by means of the Walsh transform of f and of the f_i's. For this purpose, the inverse Walsh transform formula is used.

$$\begin{aligned}\widehat{\chi_F}(u_1, \ldots, u_k) &= \sum_{(x_1,\ldots,x_k)} \frac{1}{2^k} \sum_{v\in\mathbb{F}_2^k} \widehat{\chi_f}(v)(-1)^{v_1 f_1(x_1)+u_1\cdot x_1+\cdots+v_k f_k(x_k)+u_k\cdot x_k} \\ &= \frac{1}{2^k} \sum_{v\in\mathbb{F}_2^k} \widehat{\chi_f}(v) \prod_{i|v_i=0} (2^{n_i}\delta_0(u_i)) \prod_{i|v_i=1} \widehat{\chi_{f_i}}(u_i)\end{aligned}$$

where δ_0 denotes the Boolean function that takes value 1 at the zero vector and 0 elsewhere. Relation (3.5) shows that the major contribution to the Walsh transform of F is the 2^{n_i} factor that appears if $u_i = 0$, and this contribution grows exponentially with the number of zero components u_i. This implies that the best linear approximations of F are heuristically those of low weights. In order to counterbalance this effect, the idea is to choose a function f with a Walsh transform that grows exponentially with the weight of the variable. In this case, a very approximate bound on the nonlinearity of F can even be obtained. Suppose that all n_i's equal n, that the Walsh transform of each f_i is bounded by M, that is, $|\widehat{\chi_{f_i}}(u_i)| \leq M$ and that there exists a constant a such that, for any vector $v \in \mathbb{F}_2^k$, one has $|\widehat{\chi_f}(v)| \leq a^{\mathrm{wt}(v)}$. For $(u_1, \ldots, u_k) \in \mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n$, let S denote the set $\{i \in \{1, \ldots, k\} \mid u_i \neq 0\}$ and s denote the cardinality of S. As the nonzero terms of sum (3.5) are those for which $v_i = 0$ implies $u_i = 0$, the summation can be limited to vectors v whose support $\mathrm{supp}(v)$ includes S. Thus,

$$\begin{aligned}|\widehat{\chi_F}(u_1, \ldots, u_k)| &\leq \frac{1}{2^k} \sum_{v|S\subset\mathrm{supp}(v)} a^{\mathrm{wt}(v)} M^{\mathrm{wt}(v)} (2^n)^{k-\mathrm{wt}(v)} \\ &\leq \frac{1}{2^k} \sum_{t=s}^{k} \binom{k-s}{t-s} (2^n)^{k-t} M^t a^t = \frac{M^s a^s}{2^k} (2^n + aM)^{k-s}\end{aligned}$$

In consequence, in some iterated cipher, a round ciphering function with an immunity profile that grows exponentially may provide a better resistance to linear cryptanalysis.

3.4.3 Almost resilient Boolean functions and φ-correlation Immune Boolean Functions

An alternative approach was proposed by Kurosawa [155] that relaxes the constraints of balancedness of the sub-functions and introduces the concept of *almost resiliency*. Each of the two approaches relies on one of the characterizations of correlation immunity that are equivalent. Consequently, it is advisable to wonder the possible connections between these two approaches. We clarify these connections in this section. We first recall the definition of almost resilient Boolean functions.

Definition 3.4.4. *[154] Let f a Boolean function defined on $\mathbb{F}_2^n$. Let t be any positive integer less than n. Let ε be any positive real less than 1. Then f is said to be ε-almost $(n,1,t)$-resilient if* $\left|\Pr\left(f(X)=y \mid X^I=\sigma\right)-\frac{1}{2}\right| \leq \varepsilon$ *for any subset $I=\{i_1,\ldots,i_t\}$ of $\{1,\ldots,n\}$ whose cardinality equals t, $\sigma \in \mathbb{F}_2^t$ and $y \in \mathbb{F}_2$. Here $\{X^I=\sigma\}$ denotes the event $\{X_{i_1}=\sigma_1,\ldots,X_{i_t}=\sigma_t\}$.*

The restrictions of an ε-almost $(n,1,t)$-resilient Boolean function f, obtained by fixing t input bits, lie at distance at most $\varepsilon 2^{n-t}$ from balanced functions. A sufficient condition for almost resiliency involving the Walsh transform has been proposed in [147].

Proposition 3.4.5 ([147, Corollary 4.1])**.** *Let f be an n-variable Boolean function, ε be a positive real and t be a positive integer less than n. Suppose that f is balanced and that, for all $\omega \in \mathbb{F}_2^n$ such that $1 \leq \mathrm{wt}(\omega) \leq t$, $\left|\widehat{\chi_f}(\omega)\right| \leq 2^{n+1}\varepsilon$. Then f is $((2^t-1)\varepsilon)$-almost $(n,1,t)$ resilient.*

This result can be stated in a much more precise way for φ-correlation immune Boolean functions. First, some notation is introduced. Let f be an n-variable Boolean function and $\sigma=(\sigma_1,\ldots,\sigma_r) \in \mathbb{F}_2^r$. For any subset $I=\{i_1,\ldots,i_r\}$ of $\{1,\ldots,n\}$, we denote by f_I^σ the sub-function on $\mathbb{F}_2^{n-r}$ obtained by setting the i_jth input to σ_j for every $j \in \{1,\ldots,r\}$. We finally recall the *Poisson summation formula* [31, Corollary 1]. Let f be a Boolean function on $\mathbb{F}_2^n$. Then, for any vector space E of $\mathbb{F}_2^n$, and any a, $b \in \mathbb{F}_2^n$, we have

$$\sum_{u \in a+E} (-1)^{b\cdot u}\widehat{\chi_f}(u) = \#E\,(-1)^{a\cdot b} \sum_{x \in b+E^\perp} (-1)^{a\cdot x+f(x)} \tag{3.5}$$

where $E^\perp=\{x \in \mathbb{F}_2^n \,/\, \forall y \in E,\, x\cdot y=0\}$ is the dual of E. We then prove

Proposition 3.4.6. *([40]) Let f be a Boolean function defined over $\mathbb{F}_2^n$ and let φ be any integer-valued mapping over $\{0,\ldots,n\}$. Assume that f is φ-correlation immune. Let $r \in \{1,\ldots,n-1\}$, $\sigma \in \mathbb{F}_2^r$ and $\{i_1,\ldots,i_r\} \subset \{1,\ldots,n\}$. Then f_I^σ is φ_r-correlation immune with $\varphi_r(k) = \frac{1}{2^r}\sum_{j=0}^r \binom{r}{j}\varphi(k+j)$, $k \in \{0,\ldots,n-r\}$.*

Proof. In this proof, $I=\{i_1,\ldots,i_r\}$ is an arbitrary subset of $\{1,\ldots,n\}$ ($r<n$), σ is an element of $\mathbb{F}_2^r$ and ω is an element of $\mathbb{F}_2^{n-r}$. Let E be the vector space whose dual equals $E^\perp=\{x \in \mathbb{F}_2^n \mid x_{i_1}=\cdots=x_{i_r}=0\}$. Let $b \in \mathbb{F}_2^n$ be such that $b_{i_j}=\sigma_j$ for every $j \in \{1,\ldots,r\}$ and 0 otherwise. Set $\{k_1,\ldots,k_{n-r}\}=\{1,\ldots,n\}\setminus\{i_1,\ldots,i_r\}$. Assume that $k_1<\cdots<k_{n-r}$. Let $a \in \mathbb{F}_2^n$ be such that $a_{k_j}=\omega_j$ for $j \in \{1,\ldots,n-r\}$ and 0 otherwise. With such notation, we have $\sum_{x\in b+E^\perp}(-1)^{a\cdot x+f(x)} = \widehat{\chi_{f_I^\sigma}}(\omega)$. Then, we deduce from the Poisson summation formula (3.5) that

$$|\widehat{\chi_{f_I^\sigma}}(\omega)| \;=\; \frac{1}{\#E}\sum_{u\in a+E}(-1)^{b\cdot u}\widehat{\chi_f}(u)\,.$$

The Hamming weights of the elements of $a+E$ range from $\mathrm{wt}(\omega)$ to $\mathrm{wt}(\omega)+r$. Therefore

$$|\widehat{\chi_{f_I^\sigma}}(\omega)| \leq \frac{1}{|E|}\times\sum_{j=0}^r\binom{r}{j}\varphi(\mathrm{wt}(\omega)+j)\,.$$

□

This proposition is a generalization of the well-known result : if a n-variable Boolean function is correlation immune of order t then any sub-function obtained by fixing r inputs with $r<t$ is $(t-r)$-th order correlation immune. We then prove thanks to this Proposition the following statement.

Proposition 3.4.7. *([40]) Let n be any integer, $n \geq 2$. Let φ be any integer-valued mapping over the set $\{1,\ldots,n\}$. Let f be a Boolean function over $\mathbb{F}_2^n$. Assume that f is φ-correlation immune. Then f is $\varepsilon_{\varphi,t}$-almost $(n,1,t)$ resilient for any positive integer t less than n where $\varepsilon_{\varphi,t} = \frac{1}{2^{n+1}} \sum_{j=1}^{t} \binom{t}{j} \varphi(j)$.*

Proof. Let $I = \{i_1,\ldots,i_t\}$ be an arbitrary subset of $\{1,\ldots,n\}$ $(t < n)$ and σ is an element of $\mathbb{F}_2^t$. Note that $\Pr\big(f(X) = y \mid X^I = \sigma\big) = \frac{1}{2} \pm \frac{\widehat{\chi_{f_I^\sigma}}(0)}{2^{n-t+1}}$. According to Proposition 3.4.6, f_I^σ is φ_t-correlation immune with $\varphi_t(k) = \frac{1}{2^t} \sum_{j=0}^{t} \binom{t}{j} \varphi(k+j)$, $k \in \{0,\ldots,n-t\}$. Therefore,

$$\big|\Pr\big(f(X) = y \mid X^I = \sigma\big) - \frac{1}{2}\big| = \frac{1}{2^{n-t+1}} \big|\widehat{\chi_{f_I^\sigma}}(0)\big| \leq \frac{1}{2^{n+1}} \sum_{j=0}^{t} \binom{t}{j} \varphi(j)\,.$$

□

Remark 3.4.8. *We obtain a better result than the one directly deduced from Proposition 3.4.5 for φ-correlation immune Boolean functions. Indeed, Proposition 3.4.5 only allows to conclude that f is $\varepsilon'_{\varphi,t}$-almost $(n,1,t)$ resilient with $\varepsilon'_{\varphi,t} = \frac{2^t-1}{2^{n+1}} \cdot \max_{j\in\{1,\ldots,t\}} (\varphi(j))$.*

3.4.4 Primary constructions of φ-correlation immune Boolean functions

Maiorana-McFarland's construction

The Maiorana-McFarland's class is the set of all n-variable Boolean functions which can be written as follows (n being a positive integer) :

$$\forall (x,y) \in \mathbb{F}_2^r \times \mathbb{F}_2^s, \quad f(x,y) = \pi(y) \cdot x \oplus g(y)\,, \tag{3.6}$$

where r and s are two positive integers such that $r+s=n$, where π is a Boolean map from $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$ and g is a s-variable Boolean function. The Walsh transform of such a Boolean function is

$$\forall (a,b) \in \mathbb{F}_2^r \times \mathbb{F}_2^s, \quad \widehat{\chi_f}(a,b) = 2^r \sum_{y\in\pi^{-1}(a)} (-1)^{b\cdot y + g(y)}\,.$$

Resilient Boolean functions whose immunity profile increases in proportion to the square root of the order can be designed from Maiorana-McFarland's class. Indeed, suppose that we can find π such that, for every $a \in \mathbb{F}_2^r$,

$$\#\pi^{-1}(a) = 0 \text{ if } \mathrm{wt}(a) \leq t \text{ and } \#\pi^{-1}(a) \leq \lambda \lfloor \sqrt{\mathrm{wt}(a)} \rfloor \text{ otherwise} \tag{3.7}$$

for some positive integer t less than r and some positive integer λ. Then any Boolean function f of the form (3.6) is φ-correlation immune with $\varphi(\ell) = 0$ if $\ell \in \{0,\ldots,t\}$, $\varphi(\ell) = 2^r \lambda \lfloor \sqrt{\ell} \rfloor$ for $\ell \in \{t+1,\ldots,r\}$ and $\varphi(\ell) = 2^r \lambda \sqrt{r}$ otherwise. The existence of such an application π requires that r, s and t fulfil the following inequality deduced from $\bigcup_{a\in\mathbb{F}_2^r, \mathrm{wt}(a)\geq t+1} \pi^{-1}(a) = \mathbb{F}_2^s$:

$$\lambda \sum_{l=t+1}^{r} \binom{r}{l} \lfloor \sqrt{\ell} \rfloor \geq 2^s\,. \tag{3.8}$$

The nonlinearity of f is greater than or equal to $2^{n-1} - 2^{r-1}\lfloor \sqrt{r} \rfloor$ and its algebraic degree equals $\max(\deg(\pi_1)+1,\ldots,\deg(\pi_r)+1, s)$. More generally, one can design ψ-correlation immune Boolean

function from the class of Maiorana-McFarland with $\psi(i) = \lambda 2^r \varphi(\min(i,r))$ for $i \in \{0,\ldots,n\}$ provided that $\lambda \sum_{l=0}^{r} \binom{r}{l} \varphi(\ell) \geq 2^s$ under the assumption $\#\pi^{-1}(a) \leq \lambda\varphi(\mathrm{wt}(a))$ for every $a \in \mathbb{F}_2^r$.

Note that it is possible to design φ-correlation immune Boolean functions from the effective partial spreads class [29] with the same nice properties. Because of length limits, we do not develop this further in the present paper.

Symmetric Boolean functions with exponential correlation immunity profile

The condition of φ-correlation immunity only deals with the weight of the argument of the Walsh transform. It is then natural to consider symmetric functions, that is, Boolean functions whose output only depends on the weight of the input vector. If f is an n-variable symmetric Boolean function (n is a positive integer), then there exists a function $\nu_f : \{0,\ldots,n\} \to \mathbb{F}_2$ such that $f(x) = \nu_f(\mathrm{wt}(x))$ for every $x \in \mathbb{F}_2^n$. In the sequel, the function ν_f is called the *simplified value vector* of the symmetric function f.

The Fourier transform of an n-variable symmetric Boolean function f is symmetric too and can be expressed by means of Krawtchouk polynomials for all $\omega \in \mathbb{F}_2^n$ by $\widehat{f}(\omega) = \sum_{k=0}^{n} \nu_f(k) K_k(\mathrm{wt}(\omega), n)$ where ν_f denotes the simplified value vector associated to f and where $K_k(X,n) = \sum_{j=0}^{n} (-1)^j \binom{X}{j}\binom{n-X}{k-j}$, $k = 0, 1, \ldots n$, are the so-called Krawtchouk polynomials{nomenclature[C]$K_k(X,n)$The so-called Krawtchouk polynomials. For every $k \in \{0,1,2\}$, we denote by $s_{k,3}$ the n-variable symmetric Boolean function whose simplified vector value $\nu_{s_{k,3}}$ is defined by $\nu_{s_{k,3}}(i) = 1$ if $i \equiv k \pmod 3$ and 0 otherwise. The values of the Fourier transform of such functions can easily be calculated. For every $u \in \mathbb{F}_2^n$, denoting $\ell = wt(u)$ and every $k \in \{0,1,2\}$, we have $\widehat{s_{k,3}}(u) = \sum_{\substack{0 \leq j \leq n \\ j \equiv k \,(mod\, 3)}} K_j(\ell, n)$. Let us denote by ω the primitive third root of unity $\omega = e^{2i\pi/3}$. Since we have $\omega^3 = 1$, we deduce that $\sum_{k=0}^{2} \omega^{ke} \widehat{s_{k,2}}(u) = \sum_{0 \leq j \leq n} \omega^{je} K_j(\ell, n)$, for every $e \in \{0,1,2\}$. The generating function of the Krawtchouk polynomials is $\sum_{k=0}^{n} K_k(w,n) z^k = (1-z)^w (1+z)^{n-w}$, for $w \in \{0,\ldots,n\}$, and $z \in \mathbb{C}$. This implies that $\sum_{k=0}^{2} \omega^{ke} \widehat{s_{k,3}}(u) = (1-\omega^e)^\ell (1+\omega^e)^{n-\ell}$. It is well-known that the inverse of the 3×3 matrix whose term at row k and column e equals ω^{ke} is the matrix whose term at row k and column e equals $\frac{1}{3}\omega^{-ke}$. Thus, For every $k \in \{0,1,2\}$ and every $u \in \mathbb{F}_2^n$, denoting $\ell = wt(u)$, the value at u of the Fourier transform $\widehat{s_{k,3}}(u)$ of the function $s_{k,3}$ equals $\frac{1}{3}\sum_{e=0}^{2} (1-\omega^e)^\ell (1+\omega^e)^{n-\ell} \omega^{-ke}$. Hence $\widehat{s_{k,3}}(u) = \frac{2}{3}\Re\left((1-\omega)^\ell (1+\omega)^{n-\ell} \omega^{-k}\right)$ (where $\Re(z)$ is the real part of $z \in \mathbb{C}$) because ω^2 is the complex conjugate of ω.

We deduce finally from $1 + \omega + \omega^2 = 0$ and $(1-\omega)\omega^{-2} = \mathrm{i} \cdot \sqrt{3}$ (where i is the primitive square root of unity in $\mathbb{C}$) that $\widehat{\chi_{s_{k,3}}}(u) = -2\widehat{s_{k,3}}(u) = (-1)^{n+1-\ell} \cdot \frac{4}{3} \cdot 3^{\frac{\ell}{2}} \cdot \Re\left(\mathrm{i}^\ell \omega^{2n-k}\right)$. Now, $\Re\left(\mathrm{i}^\ell \omega^{2n-k}\right)$ equals ± 1 if ℓ is even and $2n - k \equiv 0 \pmod 3$, $\pm\frac{1}{2}$ if ℓ is even and $2n - k \not\equiv 0 \pmod 3$, 0 if ℓ is odd and $2n - k \equiv 0 \pmod 3$, $\pm\frac{\sqrt{3}}{2}$ if ℓ is odd and $2n - k \not\equiv 0 \pmod 3$. Then the n-variable symmetric Boolean functions $s_{k,3}$, $k \in \{0,1,2\}$, are φ-correlation immune where φ is the integer valued mapping over $\{0,\ldots,n\}$ defined by $\varphi(i) = 4 \cdot 3^{\lfloor \frac{i-1}{2} \rfloor}$ for every $i \in \{1,\ldots,n\}$ and $\varphi(0) = 2^n$.

3.4.5 Secondary constructions of φ-correlation immune Boolean functions

The generalized Tarannikov et *al.* construction

A series of secondary constructions of highly nonlinear resilient functions has been proposed in the literature. This series has led to the very general following construction [**?**] : Let r, s, t and m be positive integers such that $t < r$ and $m < s$. Let f_1 and f_2 be two r-variable t-resilient functions. Let g_1 and g_2 be two s-variable m-resilient functions. Then the function $h(x,y) = f_1(x) \oplus g_1(y) \oplus$

$(f_1 \oplus f_2)(x)\,(g_1 \oplus g_2)(y)$, $x \in F_2^r, y \in F_2^s$ is an $(r+s)$-variable $(t+m+1)$-resilient function. The Walsh transform of h takes value $\widehat{\chi_h}(a,b) = \frac{1}{2}\widehat{\chi_{f_1}}(a)\,[\widehat{\chi_{g_1}}(b) + \widehat{\chi_{g_2}}(b)] + \frac{1}{2}\widehat{\chi_{f_2}}(a)\,[\widehat{\chi_{g_1}}(b) - \widehat{\chi_{g_2}}(b)]$. Assume then that f_1 and f_2 (resp. g_1 and g_2) are φ-correlation immune (resp. φ'-correlation immune), where φ and φ' are exponential, say $\varphi(\ell) = \lambda 2^{\beta\ell}$ and $\varphi'(\ell) = \lambda' 2^{\beta'\ell}$. Then, since $wt(a,b) = wt(a) + wt(b)$, h is φ''-correlation immune with $\varphi''(\ell) = 2\lambda\lambda' 2^{(\beta+\beta')\ell}$. Note that if $f_1 = f_2$ or $g_1 = g_2$, that is, in the case of a *direct sum*, we have $\varphi''(\ell) = \lambda\lambda' 2^{(\beta+\beta')\ell}$.

A recent secondary construction without extension of the number of variables

Given three Boolean functions f_1, f_2 and f_3, there is a nice relationship between their Walsh transforms and the Walsh transforms of two of their elementary symmetric related functions [29]: let us denote by σ_1 the Boolean function equal to $f_1 \oplus f_2 \oplus f_3$ and by σ_2 the Boolean function equal to $f_1 f_2 \oplus f_1 f_3 \oplus f_2 f_3$; then we have $f_1 + f_2 + f_3 = \sigma_1 + 2\sigma_2$ (where these additions are calculated in the ring of integers, that is, not mod 2). This implies $\widehat{\chi_{f_1}} + \widehat{\chi_{f_2}} + \widehat{\chi_{f_3}} = \widehat{\chi_{\sigma_1}} + 2\widehat{\chi_{\sigma_2}}$. If f_1, f_2 and f_3 are k-th order correlation immune (resp. k-resilient), then σ_1 is k-th order correlation immune (resp. k-resilient) if and only if σ_2 is k-th order correlation immune (resp. k-resilient). Moreover, if f_1, f_2 and f_3 are φ-correlation immune as well as σ_1, then, σ_2 is 2φ-correlation immune, whatever is φ. This construction of σ_2 from f_1, f_2, f_3 and σ_1 has the interest of increasing the algebraic complexity of the functions (e.g. their algebraic immunity) without decreasing their nonlinearity (see [29]).

3.5 On the number of Boolean functions satisfying some criteria: number of resilient functions

It is important to ensure that the selected criteria do not restrict the choice of fonction too severely that is, the set of functions must be enumerated. Theoretical and pratical studies reveal criteria that functions must satisfy. Given specific criteria it is important to know that there exist suitable numbers of functions satisfying them. As a result the problem arises of enumerating sets of functions satisfying various criteria or even (as a start point) satisfying one criterion. But this enumeration is unknown for most criteria. In the following we discuss on the number of resilient Boolean functions that is Boolean functions which are both balanced and m-correlation immune. The problem of counting the number of m-resilient n-variable Boolean functions is still challenging. Indeed, this number is only known for $m = 1$ up to 7 variables (the number of 1-resilient 7-variable Boolean function has been found in 2007 [3]) and for $m \geq n - 3$ for every n [17]. This problem seems to be untractable.

In fact, the problem of efficiently bounding from below and from above the number of m-resilient n-variable Boolean functions remains also open for every positive integer m less than $n-3$. Schneider [231] obtained an upper bound which seems efficient for resilient functions of low order. Some other results have been obtained in [117, 240, 274]. Their results are slightly better than [231] but are more complex to compute. Schneider's upper bound has been improved for high order in [37, 42]. None of the upper bounds presented in [37, 42, 231] improves upon all the other upper bounds in all situations. Few efficient lower bounds were found. Mostly, they are obtained by building and counting restricted classes of resilient Boolean functions [177, 205, 240, 269]. Recently, further improvement has been done by Le Bars and Viola [3] who presented the best lower bound and upper bound on the number of 1-resilient n-variable Boolean function. In this section, we present an approach for the problem of counting the number m-resilient n-variable Boolean functions.

In the following, $\{1, \ldots, n\}$ stands for the set of all integers ranging from 1 to n and $\mathcal{P}_n$ stands

for the set of subsets of $\{1,\ldots,n\}$. The cardinality of a subset I of $\{1,\ldots,n\}$ shall be denoted by $\#I$. We denote by Θ_n^m the subset of $\mathcal{P}_n$ of all subsets whose cardinality is at most $n-m-1$. We let Γ_n^m be the subset of $\mathcal{P}_n$ formed with all subsets of $\{1,\ldots,n\}$ of cardinality at least $n-m$. The set of all n-variable m-resilient Boolean functions shall be denoted by Res_n^m. It has been shown that the higher the order of resiliency is, the lower the maximum degree is. More precisely, it has been shown :

Proposition 3.5.1. *([236]) Suppose that $1 \leq m < n-1$. Then, the algebraic degree of an n-variable m-resilient Boolean function is at most $n-m-1$.*

Recall that any n-variable Boolean function can be viewed as an integer-valued mapping taking values in the subset $\{0,1\}$ of $\mathbb{Z}$ and that any integer-valued mapping f can be uniquely represented (the Numerical Normal form) as a multivariate polynomial over $\mathbb{Z}$:

$$\forall x \in \mathbb{F}_2^n, \quad f(x) = \sum_{I \in \mathcal{P}_n} \lambda_I \prod_{i \in I} x_i \tag{3.9}$$

where the λ_I's are in $\mathbb{Z}$. Recall that the degree of the numerical normal form of an integer-valued map f is called its numerical degree. To ensure that f takes values in $\{0,1\}$, that is, that satisfies $f^2(x) = f(x)$ for every $x \in \mathbb{F}_2^n$, the coefficients λ_I's has to satisfy

$$\forall I \in \mathcal{P}_n, \quad \Big(\sum_{J \subset I} \lambda_J\Big)^2 - \sum_{J \subset I} \lambda_J = 0. \tag{3.10}$$

where $\sum_{J \subset I}$ denotes the summation over all the subsets J of $\{1,\ldots,n\}$ which are contained in the subset I. Carlet and Guillot ([39]) have characterized resilient Boolean function by means of the numerical normal form. We give below this characterization.

Theorem 3.5.2. *([39]) Let f be an n-variable Boolean function f. Let g be the n-variable Boolean function defined as : $\forall x \in \mathbb{F}_2^n$, $g(x) = f(x) \oplus \bigoplus_{i=1}^n x_i$. Then, f is m-resilient if and only if the numerical degree of g is less than or equal to $n-m-1$.*

3.5.1 State of art on the number of resilient Boolean functions

In this subsection, we present a short and non exhaustive survey of the question of counting or finding lower bound or upper bound for the number of m-resilient n-variable Boolean functions. We omit to speak about the lower bounds. In fact, they are mostly obtained by building classes of m-resilient n-variable Boolean function. For further details, we send the reader to [31] which summarizes the previous known results related with the enumeration of resilient Boolean function.

The only n-variable Boolean functions which are $(n-1)$-resilient are the two affine n-variable Boolean functions : $\bigoplus_{i=1}^n x_i$ and its complement $1 \oplus \bigoplus_{i=1}^n x_i$. Thus, $\#Res_n^{n-1} = 2$. Siegenthaler's upper bound on the algebraic degree of a resilient Boolean function (Proposition 3.5.1) implies that only affine n-variable affine Boolean functions can be $(n-2)$-resilient. Now, a sub-function obtained by fixing at most $n-2$ input bits in an affine Boolean function stays balanced if and only if this sub-function is not constant. That requires that the algebraic normal form of this function contains at least $n-1$ monomials x_i. The number of such affine n-variable Boolean functions equals $2\binom{n}{n-1} + 2$, that is, we have $\#Res_n^{n-2} = 2(n+1)$. The first non trivial result about the number of m-resilient Boolean functions has been obtained by Camion and *al* ([17]) :

$$\#Res_n^{n-3} = \frac{n(n-1)(3n-2)(n+1)}{3}$$

Except those cases, the only other known values are the ones of $\#Res_5^1$, $\#Res_6^1$ (Harary and Palmer, [120]) and $\#Res_7^1$ (Le Bars and Viola, [3]) :

$$\#Res_5^1 = 807980 \quad \#Res_6^1 = 95259103924394$$
$$\#Res_7^1 = 234780157547888544394976226892 96$$

For the other values of $\#Res_n^m$, upper bounds have been shown. Before stating those uppers bounds, let us make a simple remark : according to Proposition 3.5.1, the algebraic degree of an n-variable m-resilient Boolean function cannot exceed $n-m-1$; that implies a simple upper bound of the number of n-variable m-resilient Boolean functions :

$$\#Res_n^m \leq 2^{1+n+\binom{n}{2}+\cdots+\binom{n}{n-m-1}} \tag{3.11}$$

that we shall refer in the sequel as the *naive bound* on the number of n-variable m-resilient Boolean function. The first general and efficiently computed upper bound was found by Schneider ([231]).

Proposition 3.5.3. *([231]). For every positive integers n and m such that $1 \leq m \leq n-1$, we have :*

$$\#Res_n^m \leq \prod_{j=1}^{n-m} \binom{2^j}{2^{j-1}}^{\binom{n-j-1}{m-1}}$$

This bound is weak for high orders of resiliency. For instance, the exact number of $(n-3)$-resilient which equals $n(n-1)(3n-2)(n+1)/3$ is much less than $\prod_{j=1}^{3} \binom{2^j}{2^{j-1}}^{\binom{n-j-1}{n-4}}$. This upper bound has been partially improved for high orders, firstly, by Carlet and Klapper and, next, by Carlet and Gouget.

Proposition 3.5.4. *([42]) For every positive integers n and m such that $1 \leq m \leq n-1$, we have :*

$$\#Res_n^m \leq \frac{2^{\sum_{i=0}^{n-m-1}\binom{n}{i}} - 2^{\sum_{i=0}^{n-m-2}\binom{n}{i}}}{2^{2^{2m+1}-1}} + 2^{\sum_{i=0}^{n-m-2}\binom{n}{i}}$$

for $2 \leq m < \frac{n}{2}$ and

$$\#Res_m^n \leq \frac{2^{\sum_{j=0}^{n-m-1}\binom{n}{j}}(1+\epsilon)}{2^{\sum_{j=0}^{n-m-1}\binom{m-1}{i}}} + 2^{\sum_{j=0}^{n-m-2}\binom{n}{j}} \text{ where } \epsilon = \frac{1}{2^{\Omega((2^n/n)^{1/2})}}.$$

for $\frac{n}{2} \leq m < n-2$.

Proposition 3.5.5. *([37]) For every positive integers n and m such that $1 \leq m \leq n-1$, we have :*

$$\#Res_m^n \leq 2^{\sum_{i=0}^{n-m-2}\binom{n}{i}} + \frac{\binom{n}{n-m-1}}{2^{\binom{m+1}{n-m-1}+1}} \prod_{i=1}^{n-m} \binom{2^j}{2^{j-1}}^{\binom{n-j-1}{m-1}}$$

3.5.2 Representation formulas for the number of resilient Boolean functions

Throughout this section, we shall use the following notation in order to allow compact description of our result. Let $\mathcal{X}$ be a set of numbers. We shall denote by $\mathcal{X}^{\mathcal{I}}$, where $\mathcal{I}$ is a finite set, the set $\{\text{span}\, xI\mathcal{I} \mid \forall I \in \mathcal{I},\, x_I \in \mathcal{X}\}$. Throughout this section, n denotes any positive integer greater

than 4 and m is a positive integer such that $m < n-3$. We shall denote by $\oint$ the Cauchy integral, that is, in the sequel, the expression $\oint F(z)dz$, where F is a k-variables complex-valued mapping and where we adopt the multivariate notation $dz = \prod_{i=1}^{k} z_i$, has to be understood as a multiple integral; each integral is over a circle of radius < 1 centered at 1; all appearing radii should be different. We shall also use the following result that expresses terms of a multi-indexed integer sequences by means of a residue formula

Proposition 3.5.6. *Let $K = (K_{n_1,\ldots,n_k})_{(n_1,\ldots,n_k)\in\mathbb{N}^k}$ be a multi-indexed integer sequence. Let G_K be the associated multivariate generating function, that is, the multivariate mapping defined as*

$$G_K(z) = \sum_{(n_1,\ldots,n_k)\in\mathbb{N}^k} K_{n_1,\ldots,n_k} \prod_{i=1}^{k} z_i^{n_i}.$$

for $z = (z_1,\ldots,z_k) \in \mathbb{C}^k$. Then, for every $n = (n_1,\ldots,n_k) \in \mathbb{N}^k$, we have

$$K_{n_1,\ldots,n_k} = \frac{1}{(2i\pi)^k} \oint G_K(z) z^{-n} \frac{dz}{z}$$

where we use the multivariate notation : $z^{-n} = \prod_{i=1}^{k} z_i^{-n_i}$ and $dz = \prod_{i=1}^{k} dz_i$.

A first representation formula

The problem of counting the number of m-resilient n-variable Boolean functions can be reworded into the problem of counting the integer solutions of a system of linear inequalities. For that, we use Theorem 3.5.2 that characterizes the n-variable Boolean function which are m-resilient by using the numerical normal form (3.9).

Proposition 3.5.7. *([194]) Let $\mathfrak{R}_n^m$ be the subset of $\mathbb{R}^{\Theta_n^m}$ defined as*

$$\mathfrak{R}_n^m = \Big\{ (x_J)_{J\in\Theta_n^m} \in \mathbb{R}^{\Theta_n^m} \;\Big|\; \forall I \in \mathcal{P}_n,\, 0 \le \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J \le 1 \Big\}. \tag{3.12}$$

Then,

$$\#Res_n^m = \#(\mathbb{Z}^{\Theta_n^m} \cap \mathfrak{R}_n^m).$$

Proof. Take $f \in \mathcal{B}_n$. Define $g \in \mathcal{B}_n$ as : $\forall x \in \mathbb{F}_2^n$, $g(x) = f(x) \oplus \bigoplus_{i=1}^{n} x_i$. By Theorem 3.5.2, f is m-resilient *if and only if* the numerical degree of g is at most $n-m-1$. Now, the map from $\mathcal{B}_n$ to itself which maps f to g is one-to-one. That implies in particular that the number of m-resilient n-variable Boolean function equals the number of integer-valued mappings taking values in $\{0,1\}$ whose numerical normal forms is of numerical degree at most $n-m-1$. Now, because of the uniqueness of the numerical normal form and according to (3.10), $\#Res_n^m$ is equal to the number of $(\lambda_J)_{J\in\Theta_n^m} \in \mathbb{Z}^{\Theta_n^m}$ which satisfies : $\forall I \in \mathcal{P}_n$, $\sum_{\substack{J\in\Theta_n^m \\ J\subset I}} \lambda_J \in \{0,1\}$. □

We now state without proof and with our notation a classical result that is called the *Mobius-Rota inversion formula*.

Lemma 3.5.8. *([194]) We have :*

$$\Big(\forall I \in \Theta_n^m,\, z_I = \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J\Big) \iff \Big(\forall I \in \Theta_n^m,\, x_I = \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} (-1)^{\#I-\#J} z_J\Big). \tag{3.13}$$

We then derive from Lemma 3.5.8 that the elements of $\mathfrak{R}_n^m$ belongs to a bounded domain of $\mathbb{R}^{\Theta_n^m}$.

Lemma 3.5.9. *([194]) Let $\mathfrak{R}_n^m$ be the subset of $\mathbb{R}^{\Theta_n^m}$ defined in Proposition 3.5.7. Let $(x_J)_{J\in\Theta_n^m} \in \mathfrak{R}_n^m$. Then $x_\emptyset \in [0,1]$ and,*

$$\forall J \in \Theta_n^m, \quad -2^{\#J-1} \leq x_J \leq 2^{\#J-1}.$$

Proof. Firstly, note that, if $I = \emptyset$, the summation $\sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J$ reduces to $x_\emptyset$ and thus the condition $0 \leq \sum_{\substack{J\in\Theta_n^m \\ J\subset\emptyset}} x_J \leq 1$ simply says that $x_\emptyset \in [0,1]$.

For the other cases, we use Lemma 3.5.8 in the particular case where $(x_J)_{J\in\Theta_n^m}$ belongs to $\mathfrak{R}_n^m$, that is, in the case where $z_I = \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J \in \{0,1\}$ for every $I \in \mathcal{P}_n$. That gives, for every $I \in \Theta_n^m$,

$$x_I = \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} (-1)^{\#I-\#J} z_J \leq \#\{J \in \Theta_n^m \mid J \subset I,\ \#I - \#J \text{ is even}\} = 2^{\#J-1}$$

and

$$x_I = \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} (-1)^{\#I-\#J} z_J \geq -\#\{J \in \Theta_n^m \mid J \subset I,\ \#I - \#J \text{ is odd}\} = -2^{\#J-1}.$$

□

Remark 3.5.10. *One can recover the* naive upper bound (3.11) *by using Mobius-Rota inversion formula* (3.13). *Indeed, introduce the linear mapping φ from $\mathbb{R}^{\Theta_n^m}$ to itself which maps $(x_J)_{J\in\Theta_n^m}$ to $\left(\sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J\right)_{J\in\Theta_n^m}$. Lemma 3.5.8 implies that φ is one-to-one. Now, by definition, the subset $\mathfrak{R}_n^m$ is contained in the preimage of $\{0,1\}^{\Theta_n^m}$ under φ. Now, the linear mapping φ being is one-to-one, we have : $\#\mathfrak{R}_n^m \leq \#\{0,1\}^{\Theta_n^m} = 2^{\#\Theta_n^m} = 2^{\sum_{j=0}^{n-m-1}\binom{n}{i}}$.*

We now use Lemma 3.5.9 to slightly reword the statement of Proposition 3.5.7. The idea is to translate $\mathfrak{R}_n^m$ by an integer vector so that its image under this translation lies in the non-negative orthant $\mathbb{R}_+^{\Theta_n^m}$. At this stage, an important point is to note that translating by an integer vector does change the integer solution count.

Corollary 3.5.11. *([194]) Let $\mathfrak{S}_n^m$ be the subset of $\mathbb{R}_+^{\Theta_n^m}$ defined as*

$$\mathfrak{S}_n^m = \left\{(y_J)_{J\in\Theta_n^m} \in \mathbb{R}_+^{\Theta_n^m} \;\middle|\; \forall I \in \mathcal{P}_n,\, b_I \leq \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} y_J \leq b_{I+1}\right\} \tag{3.14}$$

where

$$b_I = \sum_{j=1}^{\min(\#I,n-m-1)} \binom{\#I}{j} 2^{j-1} \text{ if } I \in \mathcal{P}_n \setminus \{\emptyset\} \text{ and } b_\emptyset = 0.$$

Then,

$$\#Res_n^m = \#(\mathbb{N}^{\Theta_n^m} \cap \mathfrak{S}_n^m).$$

Proof. Define $(v_J)_{J\in\mathcal{P}_n}$ as : $v_\emptyset = 0$ and, for every $J \in \mathcal{P}_n \setminus \{\emptyset\}$, $v_J = 2^{\#J-1}$. Set $\mathfrak{S}_n^m = \{(y_J) \in \mathbb{R}^{\Theta_n^m} \mid \exists (x_J)_{J\in\Theta_n^m} \in \mathfrak{R}_n^m, \forall J \in \mathcal{P}_n, y_J = x_J + v_J\}$. Lemma 3.5.9 says that $\mathfrak{S}_n^m \subset \mathbb{R}_+^{\Theta_n^m}$ since : $\forall J \in \Theta_n^m$, $x_J \geq -2^{\#J-1} = -v_J$. Now, replacing x_J by $y_J - v_J$ in all the linear inequalities defining $\mathfrak{R}_n^m$ yields to the new system of linear inequalities whose unknowns are the y_J's

$$\forall I \in \mathcal{P}_n, \quad \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} v_J \leq \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} y_J \leq \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} v_J + 1.$$

The result follows then from the identity $\sum_{\substack{J\in\Theta_n^m \\ J\subset I}} v_J = b_{\#I}$. □

Let $\mathfrak{S}_n^m$ be the subset of $\mathbb{R}_+^{\Theta_n^m}$ defined by Corollary 3.5.11. We then split $\mathfrak{S}_n^m$ into disjoint subsets. For that, we introduce a collection of subsets of $\mathbb{R}_+^{\Theta_n^m}$ indexed by $\mathbb{N}^{\mathcal{P}_n}$ whose terms are defined as

$$\forall c = (c_I)_{I\in\mathcal{P}_n} \in \mathbb{N}^{\mathcal{P}_n}, \quad \mathfrak{T}_n^{c,m} = \{(y_J)_{J\in\Theta_n^m} \in \mathbb{R}_+^{\Theta_n^m} \mid \forall I \in \mathcal{P}_n, \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} y_J = c_I\}.$$

We then have

$$\mathfrak{S}_n^m = \bigcup_{\epsilon\in\{0,1\}^{\mathcal{P}_n}} \mathfrak{T}_n^{b+\epsilon,m}. \tag{3.15}$$

where the terms of $b = (b_I)_{I\in\mathcal{P}_n}$ are the b_I's defined in Corollary 3.5.11. Next, let $K = (K_c)_{c\in\mathbb{N}^{\mathcal{P}_n}}$ be the integer sequence index by $\mathcal{P}_n$ whose terms are : $\forall c \in \mathbb{N}^{\mathcal{P}_n}$, $K_c = \#(\mathbb{N}^{\Theta_n^m} \cap \mathfrak{T}_n^{c,m})$. But above, we have

$$\#Res_n^m = \#(\mathbb{N}^{\Theta_n^m} \cap \mathfrak{S}_n^m) = \sum_{\epsilon\in\{0,1\}^{\mathcal{P}_n}} \#\mathfrak{T}_n^{b+\epsilon,m} \cap \mathbb{N}^{\Theta_n^m} = \sum_{\epsilon\in\{0,1\}^{\mathcal{P}_n}} K_{b+\epsilon}. \tag{3.16}$$

A classical approach in enumerative combinatorics is to introduce the multivariate generating function associated to K that we denote by G_K and that is defined as :

$$z \in \mathbb{C}^{\mathcal{P}_n}, \quad G_K(z) = \sum_{c\in\mathbb{N}^{\Theta_n^m}} K_c z^c \tag{3.17}$$

where we use the multivariate notation $z^c = \prod_{I\in\mathcal{P}_n} z_I^{c_I}$ for $z = (z_I)_{I\in\mathcal{P}_n}$ and $c = (c_I)_{I\in\mathcal{P}_n}$. We then prove the following key result.

Proposition 3.5.12. *([194]) The power series* (3.17) *converges provided that, for every $I \in \mathcal{P}_n$, the modulus $|z_I|$ is small enough. Moreover, when the power series converges, we have*

$$G_K(z) = \prod_{J\in\Theta_n^m} \frac{1}{1 - \prod_{\substack{I\in\mathcal{P}_n \\ J\subset I}} z_I}.$$

Proof. Firstly

$$\sum_{\mathbf{c}\in\mathbb{N}^{\mathcal{P}_n}} K_c z^c = \sum_{\mathbf{c}\in\mathbb{N}^{\mathcal{P}_n}} \sum_{y\in\mathbb{N}^{\Theta_n^m}\cap\mathfrak{T}_n^{c,m}} \prod_{I\in\mathcal{P}_n} \prod_{\substack{J\in\Theta_n^n \\ J\subset I}} z_I^{y_J}$$

because

$$z^{\mathbf{c}} = \prod_{I\in\mathcal{P}_n} z_I^{c_I} = \prod_{I\in\mathcal{P}_n} z_I^{\sum_{\substack{J\in\Theta_n^m \\ J\subset I}} y_J} = \prod_{I\in\mathcal{P}_n} \prod_{\substack{J\in\Theta_n^m \\ J\subset I}} z_I^{y_J}$$

whenever $y = (y_I)_{I\in\mathcal{P}_n} \in \mathfrak{T}_n^{c,m}$. Thus

$$\sum_{c\in\mathbb{N}^{\mathcal{P}_n}} K_c z^c = \sum_{y\in\mathbb{N}^{\Theta_n^m}} \prod_{J\in\Theta_n^m} \prod_{\substack{I\in\mathcal{P}^n\\ J\subset I}} z_I^{y_J} = \prod_{J\in\Theta_n^m} \left(\sum_{y_J=0}^{+\infty} \prod_{\substack{I\in\mathcal{P}^n\\ J\subset I}} z_I^{y_J} \right)$$
$$= \prod_{J\in\Theta_n^m} \frac{1}{1-\prod_{\substack{I\in\mathcal{P}^n\\ J\subset I}} z_I}$$

provided that, for every $I \in \mathcal{P}_n$, $\left|\prod_{\substack{I\in\mathcal{P}^n\\ J\subset I}} z_I\right| = \prod_{\substack{I\in\mathcal{P}^n\\ J\subset I}} |z_I|$ is small enough. A sufficient condition is that, for every $I \in \mathcal{P}_n$, $|z_I|$ is small enough. □

We finally deduce from Proposition 3.5.6 a representation formula for $\#Res_n^m$

Lemma 3.5.13. *([194]) we have*

$$\forall c \in \mathbb{N}^{\mathcal{P}_n}, \quad K_c = \frac{1}{(2i\pi)^{2^n}} \oint G_K(z) z^{-c} \frac{dz}{z}.$$

where adopt the multivariate notation $dz = \prod_{I\in\mathcal{P}_n} dz_I$.

A straightforward consequence of the preceding Lemma is a representation formula for $\#Res_m^n$.

Proposition 3.5.14. *([194]) We have*

$$\#Res_n^m = \frac{1}{(2i\pi)^{2^n}} \oint G(z) \frac{dz}{z} \tag{3.18}$$

where G is defined for $z = (z_I)_{I\in\mathcal{P}_n}$ as

$$G(z) = \prod_{I\in\mathcal{P}_n} (1+z_I) z_I^{-b_I-1} \cdot \prod_{J\in\Theta_n^m} \frac{1}{1-\prod_{\substack{I\in\mathcal{P}^n\\ J\subset I}} z_I}.$$

Proof. Replacing each term $K_{b+\epsilon}$ by its expression given by Lemma 3.5.13 in (3.16) yields to

$$\#\mathbb{N}^{\Theta_n^m} \cap \mathfrak{S}_n^m = \sum_{\epsilon\in\{0,1\}^{\mathcal{P}_n}} \frac{1}{(2i\pi)^{2^n}} \oint F(z) z^{-(b+\epsilon)} \frac{dz}{z}.$$

Exchange the summation $\sum$ and the integration $\oint$:

$$\#\mathbb{N}^{\Theta_n^m} \cap \mathfrak{S}_n^m = \frac{1}{(2i\pi)^{2^n}} \oint F(z) z^{-b} \left(\sum_{\epsilon\in\{0,1\}^{\mathcal{P}_n}} z^{-\epsilon} \right) \frac{dz}{z}.$$

We then get the result by noting that

$$\sum_{\epsilon\in\{0,1\}^{\mathcal{P}_n}} z^{-\epsilon} = \prod_{I\in\mathcal{P}_n} z_I^{-1} \sum_{\epsilon\in\{0,1\}^{\mathcal{P}_n}} z^{\epsilon} = \prod_{I\in\mathcal{P}_n} z_I^{-1} \cdot \prod_{I\in\mathcal{P}_n} (1+z_I).$$

□

A second representation formula for the number of resilient Boolean functions

In this subsection, we state an alternative representation formula for $\#Res_m^n$. To this end, we begin with noting that the set $\mathfrak{R}_n^m$ of Proposition 3.5.7 can be written as

$$\mathfrak{R}_n^m = \mathfrak{R}_n^{1,m} \cap \mathfrak{R}_n^{2,m} \tag{3.19}$$

where

$$\mathfrak{R}_n^{1,m} = \Big\{ (x_J)_{J\in\Theta_n^m} \in \mathbb{R}^{\Theta_n^m} \,\Big|\, \forall I \in \Theta_n^m,\, 0 \le \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J \le 1 \Big\}$$

and

$$\mathfrak{R}_n^{2,m} = \Big\{ (x_J)_{J\in\Theta_n^m} \in \mathbb{R}^{\Theta_n^m} \,\Big|\, \forall I \in \Gamma_n^m,\, 0 \le \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J \le 1 \Big\}.$$

Thus,

$$\mathfrak{R}_n^m \cap \mathbb{Z}^{\Theta_n^m} = \big(\mathfrak{R}_n^{1,m} \cap \mathbb{Z}^{\Theta_n^m}\big) \cap \mathfrak{R}_n^{2,m} \tag{3.20}$$

Then, consider again the linear mapping φ introduced in Remark 3.5.10, that is, let φ be the linear mapping from $\mathbb{R}^{\Theta_n^m}$ to itself which maps $(x_J)_{J\in\Theta_n^m}$ to $\left(\sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J\right)_{J\in\Theta_n^m}$. We then have $\mathfrak{R}_n^{1,m} \cap \mathbb{Z}^{\Theta_n^m} = \Big\{ x = (x_J)_{J\in\Theta_n^m} \in \mathbb{R}^{\Theta_n^m} \,\Big|\, \forall I \in \Theta_n^m,\, \varphi(x) \in \{0,1\}\Big\} = \varphi^{-1}\big(\{0,1\}^{\Theta_n^m}\big)$. Now, Mobius-Rota inversion formula recalled in Lemma 3.5.8 implies that φ is one-to-one. We thus deduce firstly that the intersection (3.19) can be rewritten as

$$\mathfrak{R}_n^m \cap \mathbb{Z}^{\Theta_n^m} = \varphi^{-1}\Big(\{0,1\}^{\Theta_n^m} \cap \varphi(\mathfrak{R}_n^{2,m})\Big) \tag{3.21}$$

but above we have

$$\#Res_n^m = \#\mathfrak{R}_n^m \cap \mathbb{Z}^{\Theta_n^m} = \#\{0,1\}^{\Theta_n^m} \cap \varphi(\mathfrak{R}_n^{2,m}). \tag{3.22}$$

We now compute the image of $\mathfrak{R}_n^{2,m}$ under φ.

Lemma 3.5.15. *([194])* $(y_J) \in \varphi(\mathfrak{R}_n^{2,m})$ *if and only if*

$$\forall I \in \Gamma_n^m, \quad 0 \le \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} (-1)^{n-m-\#J-1} \binom{\#I-\#J-1}{n-m-\#J-1} y_J \le 1.$$

Proof. Take $y = (y_J)_{J\in\Theta_n^m} \in \varphi(\mathfrak{R}_n^{2,m})$. By definition there exists $x = (x_J)_{J\in\Theta_n^m}$ such that

$$\forall I \in \Gamma_n^m, \quad 0 \le \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J \le 1 \tag{3.23}$$

and such that

$$\forall I \in \Theta_n^m, \quad y_I = \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J.$$

Mobius-Rota inversion formula (Lemma 3.5.8) implies that

$$\forall I \in \Theta_n^m, \quad x_I = \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} (-1)^{\#I-\#J} y_J.$$

Thus,

$$\begin{aligned}\forall I \in \Gamma_n^m, \quad \sum_{\substack{J\in\Theta_n^m\\ J\subset I}} x_J &= \sum_{\substack{J\in\Theta_n^m\\ J\subset I}} \sum_{\substack{K\in\Theta_n^m\\ K\subset J}} (-1)^{\#J-\#K} y_K \\ &= \sum_{\substack{K\in\Theta_n^m\\ K\subset I}} y_K \sum_{\substack{J\in\Theta_n^m\\ K\subset J\subset I}} (-1)^{\#J-\#K}.\end{aligned} \tag{3.24}$$

Now,

$$\sum_{\substack{K\in\Theta_n^m\\ K\subset J\subset I}} (-1)^{\#J-\#K} = \sum_{j=\#K}^{n-m-1} (-1)^{j-\#K} \binom{\#I-\#K}{j-\#K}$$

The result follows then from the identity : for every positive integers $1 < p < n$, we have

$$\sum_{j=0}^{p} (-1)^j \binom{n}{j} = (-1)^p \binom{n-1}{p}.$$

Indeed, if we use the Pascal identity, that is, the identity $\binom{n}{j} = \binom{n-1}{j-1} + \binom{n-1}{j}$ then we get

$$\sum_{j=0}^{p} (-1)^j \binom{n}{j} = \sum_{j=0}^{p} (-1)^j \binom{n-1}{j} + \sum_{j=0}^{p-1} (-1)^{j+1} \binom{n-1}{j}$$

Hence, all the terms at the right-hand side cancel out except the last one, that is, the term $(-1)^p \binom{n-1}{p}$. □

Combining (3.22) and Lemma 3.5.15, we get

Proposition 3.5.16. *([194]) $\#Res_n^m$ equals the number of elements (y_J) in $\{0,1\}^{\Theta_n^m}$ which satisfy*

$$\forall I \in \Gamma_n^m, \quad 0 \le \sum_{\substack{J\in\Theta_n^m\\ J\subset I}} (-1)^{n-m-\#J-1} \binom{\#I-\#J-1}{n-m-\#J-1} y_J \le 1.$$

We slightly reword the preceding proposition

Corollary 3.5.17. *([194]) $\#Res_n^m$ equals the number of elements (z_J) in $\{0,1\}^{\Theta_n^m}$ which satisfy*

$$\forall I \in \Gamma_n^m, \quad b_I \le \sum_{\substack{J\in\Theta_n^m\\ J\subset I}} \binom{\#I-\#J-1}{n-m-\#J-1} z_J \le b_I + 1$$

where

$$\forall I \in \Gamma_n^m, \quad b_I = \sum_{\substack{j=0\\ n-m-1-j \text{ is odd}}}^{n-m-1} \binom{\#I}{j} \binom{\#I-j-1}{n-m-1-j}.$$

Proof. The proof follows from the change of variables : $z_J = y_J$ if $n-m-\#J-1$ is even and $z_J = 1 - y_J$ otherwise. □

We now deduce from Corollary 3.5.17 that $\#Res_n^m$ can be interpreted as a coefficient of a multivariate polynomial.

Proposition 3.5.18. *([194])*

$$\#Res_n^m = \frac{1}{(2i\pi)^{\#\Gamma_n^m}} \oint P(z) \prod_{I\in\Gamma_n^m} z_I^{-(b_I+1)} \frac{dz}{z}$$

where P is the multivariate polynomial defined as

$$\forall z \in \mathbb{C}, \quad P(z) = \prod_{I\in\Gamma_n^m} (1+z_I) \prod_{J\in\Theta_n^m} \left(1 + \prod_{\substack{I\in\Gamma_n^m \\ J\subset I}} z_I^{a_{I,J}}\right)$$

with

$$\forall (I,J) \in \Gamma_n^m \times \Theta_n^m, \quad a_{I,J} = \binom{\#I - \#J - 1}{n-m-\#J-1}.$$

Proof. Note that

$$\prod_{I\in\Gamma_n^m} (1+z_I) \prod_{J\in\Theta_n^m} \left(1 + \prod_{\substack{I\in\Gamma_n^m \\ J\subset I}} z_I^{a_{I,J}}\right) = \prod_{I\in\Gamma_n^m} \left(\sum_{\epsilon_I=0}^{1} z^{\epsilon_I}\right) \prod_{J\in\Theta_n^m} \left(\sum_{\eta_J=0}^{1} z_I^{\eta_J a_{I,J}}\right)$$

$$= \sum_{(\epsilon,\eta)\in\{0,1\}^{\Gamma_n^m\times\Theta_m^n}} \prod_{I\in\Gamma_n^m} z_I^{\sum_{I\in\Gamma_n^m}\epsilon_I + \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} a_{I,J}\eta_J}$$

Now, the coefficient of the monomial $\prod_{I\in\Gamma_n^m} z_I^{b_I+1}$ is

$$\sum_{\epsilon\in\{0,1\}^{\Gamma_n^m}} \#\{\eta = (\eta_J)_{J\in\Theta^n} \in \{0,1\}^{\Theta^n} \mid \forall I \in \Gamma_n^m, \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} a_{I,J}\eta_J = b_I + \epsilon_I\},$$

where $a_{I,J} = \binom{\#I-\#J-1}{n-m-\#J-1}$, which is equal to $\#Res_n^m$ according to Corollary 3.5.17. The result follows then from Proposition 3.5.6. □

To conclude this section, adopting an approach of enumerative combinatorics we derived two representation formulas for the number of m-resilient n-variable Boolean functions in terms of the Cauchy integral. Nevertheless, the problem of counting the number of m-resilient n-variable Boolean functions is still challenging. In 2010, Canfield et al.[18] have obtained an asymptotic estimatimation of the number of n-variable m correlation immune Boolean functions. Their asymptotic enumeration holds if m increases with n within generous limits and specialises to functions with a given weight, including the resilient functions. In the case of $m = 1$, their estimations are valid for all weights.

3.6 The higher order nonlinearity of Boolean functions with prescribed algebraic immunity

In this section, we are interested in two cryptographic parameters. The first one is the algebraic immunity of a Boolean function which quantifies the resistance to the standard algebraic attack

of the pseudo-random generators using it as a nonlinear function. Recall that the algebraic immunity of a Boolean function f is defined as follows.

Definition 3.6.1 (Algebraic immunity)**.** *Let f be an n-variable Boolean function. An n-variable Boolean function g is said to be an* annihilator *of f if the product $f \cdot g$ is null (that is, the support of g is included in the support of $1 \oplus f$). We denote by $An(g)$ the vector space of all annihilators of g. The algebraic immunity of f is the minimum algebraic degree of all the nonzero annihilators of f or of $f \oplus 1$. The* algebraic immunity *of f is denoted by $AI(f)$.*

The second parameter is the r th-order nonlinearity which generalizes the standard nonlinearity and is thus an important parameter in cryptography, (which equals the minimum distance between any Boolean function f and the set of all Boolean function in n variable of algebraic degree at most r) and measures the capacity for resisting low-degree approximation attack [152, 234]. More precisely, the *rth order nonlinearity* is defined as follows.

Definition 3.6.2 (rth-order nonlinearity)**.** *Let f be an n-variable Boolean function. Let r be a positive integer such that $r \leq n$. The* r-th order nonlinearity *of f is the minimum Hamming distance between f and all n-variable Boolean functions from the set of all the n-variable Boolean functions of algebraic degree at most r. We shall denote the r-th order nonlinearity of f by $nl_r(f)$.*

Carlet introduced in [30] the term of *nonlinearity profile* of Boolean functions, which is the sequence whose rth-order term equals the rth-order nonlinearity of the function that we denote by $nl_r(f)$. This parameter extends the standard (first-order) nonlinearity $nl(f)$ of a Boolean function f. Several papers [72, 113, 137, 152, 204] have shown the role played by this parameter in relation to some cryptanalyses (note that contrary to the (first-order) nonlinearity, it must have low value for allowing the attacks to be realistic). Computing theoretically and algorithmically the rth-order nonlinearity of an n-variable Boolean function is a hard task for $r > 1$. Therefore the knowledge of upper and lowers bounds for the rth-order nonlinearity on a particular class of Boolean functions is important.

Lobanov's result [5] on the nonlinearity has been extended to the rth-order nonlinearity $nl_r(f)$ of an n-variable Boolean function f in two different lower bounds [30, 34]. None of the two lower bounds improves upon the other one in all situations. Indeed, the bound of [30] is better than the bound of [34] for all values of $AI(f)$ when the number of variables is smaller than or equal to 12, and for most values of $AI(f)$ when the number of variables is smaller than or equal to 22.

These lower bounds say that the rth-order nonlinearity of an n-variable Boolean function f of algebraic immunity k is greater than or equal to the maximum value between $\sum_{i=0}^{k-r-1} \binom{n}{i}$ and $\max_{r' \leq n}(\min(\lambda_{r'}, \mu_{r'}))$ where $\lambda_{r'} = 2\max\left(\sum_{i=0}^{r'-1} \binom{n}{i}, \sum_{i=0}^{k-r-1} \binom{n-r}{i}\right)$ if $r' \leq k-r-1$ and $2\sum_{i=0}^{k-r-1} \binom{n}{i}$ if $r' > k-r-1$, $\mu_{r'} = \sum_{i=0}^{k-r-1} \binom{n-r}{i} + \sum_{i=0}^{k-r'} \binom{n-r'+1}{i}$.

In this section, we show how we can improve further the lower bound of [34] for all orders and the lower bound of [30] for low orders (which are the most important from a practical point of view) : for every n-variable Boolean function f, we prove that the rth-order nonlinearity $nl_r(f)$ of a n-variable Boolean function of algebraic immunity k is greater than or equal to $\sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$. This and, we begin by studying more deeply than [30] the structure of vector spaces of annihilators with prescribed algebraic degrees for all Boolean functions.

[5] We mean, the lower bound of Lobanov:nl$(f) \geq 2^{n-1} - \binom{n}{\lfloor \frac{n}{2} \rfloor}$

3.6.1 Some results on the dimension of the vector space of prescribed degree annihilators of a Boolean function

An important parameter for evaluating the complexity of algebraic attacks on the systems using a given Boolean function is the number of linearly independent low degree annihilators of this Boolean function g and of the function $g \oplus 1$. We shall see in the next Section that it plays also an important role in relation to the r-th order nonlinearity.

Definition 3.6.3. *Let g be a Boolean function and let k be a positive integer. We denote by $An_k(g)$ the vector space of those annihilators of degrees at most k of g and by $d_{k,g}$ the dimension of $An_k(g)$.*

The dimension $d_{k,g}$ is an affine invariant, that is, we have $d_{k,g} = d_{k,g\circ A}$ for every affine automorphism A of $\mathbb{F}_2^n$ (this comes from the affine invariance of the algebraic degree and the fact that p is an annihilator of g if and only if $p \circ A$ is an annihilator of $g \circ A$). Little is known on the behavior of $d_{k,g}$. Carlet [30] proved the following upper bound on $d_{k,g}$.

Proposition 3.6.4. *([30]) For every n-variable Boolean function g of algebraic degree at most r, we have $d_{k,g} \leq \sum_{i=0}^{k} \binom{n}{i} - \sum_{i=0}^{k} \binom{n-r}{i}$. This upper bound is achieved with equality by the indicators of an $(n-r)$-dimensional affine subspace of $\mathbb{F}_2^n$ for which the dimension $d_{k,g}$ is exactly equal to $\sum_{i=0}^{k} \binom{n}{i} - \sum_{i=0}^{k} \binom{n-r}{i}$*

We can derive from this upper bound a lower bound on $d_{k,g}$. Let us introduce some notation before. For every n-variable Boolean function g and every positive integer k, we denote by $Mul_k(g)$ the vector space of all n-variable Boolean functions p that can be written as $p = gh$ where h is of algebraic degree at most k. There exists a simple relation between $d_{k,g}$ and $\dim Mul_k(g)$.

Lemma 3.6.5. *([193]) Let g be an n-variable Boolean function of algebraic degree r. Let k be any positive integer less than n. Then $\dim Mul_k(g) = \sum_{i=0}^{k} \binom{n}{i} - d_{k,g}$.*

Proof. Let ϕ_g be the linear map from $\mathcal{RM}(k,n)$ to $Mul_k(g)$ which maps h to gh. This linear map is onto and its kernel equals $An_k(g)$. Thus, by applying the rank theorem to ϕ_g, one gets that $\dim \mathcal{RM}(k,n) = \sum_{i=0}^{k} \binom{n}{i} = \dim \mathrm{Im}(\phi_g) + \dim \ker(\phi_g) = \dim Mul_k(g) + d_{k,g}$. □

The upper bound of [30] (that we have recalled in Proposition 3.6.4) and Lemma 3.6.5 lead us to a lower bound on $d_{k,g}$ achieved by the complements of the indicators of affine subspaces of $\mathbb{F}_2^n$. More precisely,

Proposition 3.6.6. *([193]) Let g be an n-variable Boolean function of algebraic degree at most r. Then, for every positive integer k, one has $d_{k,g} \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$. If g is the complement of the indicator of an $(n-r)$-dimensional affine subspace of $\mathbb{F}_2^n$ then $d_{k,g} = \sum_{i=0}^{k-r} \binom{n-r}{i}$.*

Proof. Let g be an n-variable Boolean function of algebraic degree at most r. We can assume that $k \geq r$ (otherwise the lower bound is trivial). Take $h \in An_r(g)$. We have $d_{k-r,h} \leq \sum_{i=0}^{k-r} \binom{n}{i} - \sum_{i=0}^{k-r} \binom{n-r}{i}$ by Proposition 3.6.4. Now, according to Lemma 3.6.5, $\dim Mul_{k-r}(h) = \sum_{i=0}^{k-r} \binom{n}{i} - d_{k-r,h}$. Thus $\dim Mul_{k-r}(h) \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$. Moreover, we have the inclusion $Mul_{k-r}(h) \subseteq An_k(g)$. Therefore, it holds that $d_{k,g} \geq \dim Mul_{k-r}(h) \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$. This latter inequality becomes an equality whenever g is the complement of an $(n-r)$-dimensional affine subspaces of $\mathbb{F}_2^n$ because it has been shown in [30] that $d_{k,g}$ is equal to $\sum_{i=0}^{k-r} \binom{n-r}{i}$ for such Boolean functions. □

We prove a result that we shall use to improve the lower bound of [30, 34]. To this aim, we need to introduce some additional notation. Given an element u of $\mathbb{F}_2^n$, we call the subset $\{i \in \{1,\ldots,n\} \mid u_i = 1\}$ the support of u, and we denote it by $supp(u)$. The Hamming weight of u, denoted by $\mathrm{wt}(u)$, is the cardinality of $supp(u)$. We shall use the partial ordering $\preceq$ on $\mathbb{F}_2^n$ defined as follows :

$$u, v \in \mathbb{F}_2^n, \quad (u \preceq v) \iff (supp(u) \subset supp(v))$$

Moreover, for every pair (u, v) of elements of $\mathbb{F}_2^n$, we denote by $u \vee v$ the element of $\mathbb{F}_2^n$ defined as: $\forall i = 1,\ldots,n$, $(u \vee v)_i = \max(u_i, v_i)$, that is, the element of $\mathbb{F}_2^n$ whose support is the union of the two supports $supp(u)$ and $supp(v)$. We say that an element u of a subset Π of $\mathbb{F}_2^n$ is a maximal element of Π with respect to the word partial ordering $\preceq$ if : $v \in \Pi$, $u \preceq v \Rightarrow v = u$. For every element u of $\mathbb{F}_2^n$, we denote by $\bar{u}$ the bitwise complement of u, that is, the element of $\mathbb{F}_2^n$ defined by : $\forall i \in \{1,\ldots,n\}, \bar{u}_i = 1 \oplus u_i$. We begin with proving the following Lemma.

Lemma 3.6.7. *([193]) Let g be an n-variable Boolean function whose algebraic normal form is : $\forall x \in \mathbb{F}_2^n$, $g(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u$. Set $\Pi = \{u \in \mathbb{F}_2^n \mid a_u = 1\}$. Let $\mathbf{u}$ be a maximal element of Π with respect to the partial ordering $\preceq$. Set $\Theta = \{v \in \mathbb{F}_2^n \mid v \preceq \bar{\mathbf{u}}\}$. Then $\{x^v \cdot g,\ v \in \Theta\}$ is a linearly independent family of $\mathcal{B}_n$.*

Proof. Let $(c_v)_{v \in \Theta}$ be a collection of elements of $\mathbb{F}_2$ such that : $\forall x \in \mathbb{F}_2^n$, $\bigoplus_{v \in \Theta} c_v x^v g(x) = 0$. Replacing g by its algebraic normal form yields to : $\forall x \in \mathbb{F}_2^n$, $\bigoplus_{(u,v) \in \Pi \times \Theta} c_v x^{u \vee v} = 0$. We now prove that, for every $v \in \Theta$, the monomial $x^{\mathbf{u} \vee v}$ appears only once in the sum $\bigoplus_{(u,v) \in \Pi \times \Theta} c_v x^{u \vee v}$. To this end, let us fix $v \in \Theta$ and let us look forward $v' \in \Theta$ and $u \in \Pi$ such that $u \vee v' = \mathbf{u} \vee v$. This requires that $\mathbf{u} \preceq u \vee v'$. The support of $\mathbf{u}$ being disjoint from the support of v', we must have $\mathbf{u} \preceq u$ which is possible only if $u = \mathbf{u}$ because $\mathbf{u}$ is a maximal element of Π with respect to the word ordering $\preceq$. The equality $u \vee v' = \mathbf{u} \vee v$ becomes $\mathbf{u} \vee v' = \mathbf{u} \vee v$ from which we deduce that $v = v'$ (since they are both disjoint from $\mathbf{u}$). We hence prove that, for every $v \in \Theta$, the monomial $x^{\mathbf{u} \vee v}$ appears only once in the sum $\bigoplus_{(u,v) \in \Pi \times \Theta} c_v x^{u \vee v}$ which vanishes for every word x in $\mathbb{F}_2^n$. That requires that $x \mapsto c_v x^{\mathbf{u} \vee v}$ is null on $\mathbb{F}_2^n$ yielding to $c_v = 0$. The element v being arbitrary, that proves that the collection $\{x^v \cdot g, v \in \Theta\}$ is a linearly independent family of $\mathcal{B}_n$. □

We then use Lemma 3.6.7 to show the following result.

Proposition 3.6.8. *([193]) Let g be an n-variable Boolean function of algebraic degree at most r and $g(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u$ be its ANF. Let k be a positive integer less than n. Set $\Pi = \{u \in \mathbb{F}_2^n \mid a_u = 1\}$. Let $\mathbf{u}$ be a maximal element of Π with respect to the partial ordering $\preceq$. Then*

1. *The vector space $An_k(g \oplus 1)$ is contained in $Mul_k(g)$.*
2. *$\dim Mul_k(g) \geq \sum_{i=k-\mathrm{wt}(\mathbf{u})+1}^{k} \binom{n-\mathrm{wt}(\mathbf{u})}{i} + d_{k,1 \oplus g}$.*

Proof.

1. Every annihilator h of $1 \oplus g$ satisfies $gh = h$ and thus is an element of $Mul_k(g)$.
2. The algebraic normal form of g can be rewritten as $g(x) = \bigoplus_{u \in \Pi} x^u$.

   Define $\Theta = \{v \in \Pi \mid v \preceq \bar{\mathbf{u}}\}$. Let Σ be the subset of Θ defined by $\Sigma = \{v \in \Theta \mid k - \mathrm{wt}(\mathbf{u}) + 1 \leq \mathrm{wt}(v) \leq k\}$ (this subset is non empty because $\max_{v \in \Theta} \mathrm{wt}(v) = n - \mathrm{wt}(\mathbf{u}) \geq n - r \geq k - r + 1$). Now, $\{x^v \cdot g, v \in \Sigma\}$ is a subfamily of $\{x^v \cdot g, v \in \Theta\}$ which is a linearly independent family of $\mathcal{B}_n$ according to Lemma 3.6.7. Thus, $\{x^v \cdot g, v \in \Sigma\}$ is also a linearly

independent family of $\mathcal{B}_n$. Moreover, every element of this family belongs to $Mul_k(g)$ since, for every $v \in \Sigma$, we have that $\mathrm{wt}(v) \leq k$.

Now, let V be the vector subspace spanned by all the Boolean functions $x^v g$ where v ranges over Σ. The vector subspace V is by construction a vector subspace of $Mul_k(g)$ and its dimension over $\mathbb{F}_2$ equals the cardinality of the family $\{x^v \cdot g, v \in \Sigma\}$, that is, its dimension equals $\sum_{i=k-\mathrm{wt}(\mathbf{u})+1}^{k} \binom{n-\mathrm{wt}(\mathbf{u})}{i}$.

We are now going to prove that the vector sum $V + An_k(1 \oplus g)$ is a direct sum of $Mul_k(g)$. The ANF of an element of V is of the form $\bigoplus_{(u,v)\in \Pi \times \Sigma} c_v x^{u \vee v}$. The algebraic degree of such a Boolean function is at least $k+1$. Indeed, for every $v \in \Sigma$, the monomial $x^{\mathbf{u}\vee v}$ appears at most once in the sum $\bigoplus_{(u,v)\in \Pi \times \Sigma} c_v x^{u \vee v}$ (see proof of Lemma 3.6.7) and is of algebraic degree $\mathrm{wt}(\mathbf{u}) + \mathrm{wt}(v) \geq k+1$. Hence, the intersection $V \cap An_k(1 \oplus g)$ is reduced to $\{0\}$ because every non null element of V is of algebraic degree at least $k+1$ while every non null element of $An_k(1 \oplus g)$ is of algebraic degree at most k. This proves that the vector sum $V + An_k(1 \oplus g)$ is a direct sum. This implies that $\dim Mul_k(g) \geq \dim V + \dim An_k(1 \oplus g) = \sum_{i=k-\mathrm{wt}(\mathbf{u})+1}^{k} \binom{n-\mathrm{wt}(\mathbf{u})}{i} + d_{k,1\oplus g}$.

□

We can deduce from the Proposition 3.6.8 the following lower bound on the difference $\dim Mul_k(g) - d_{k,1\oplus g}$ valid for every Boolean function of degree at most r.

Corollary 3.6.9. *Let k be a positive integer. Then, for every n-variable Boolean function g of algebraic degree at most r, we have*

$$\dim Mul_k(g) - d_{k,1\oplus g} \geq \sum_{i=k-r+1}^{k} \binom{n-r}{i}$$

Proof. Assume that the algebraic normal form of g is : $\forall x \in \mathbb{F}_2^n$, $g(x) = \bigoplus_{u\in\mathbb{F}_2^n} a_u x^u$. Set $\Pi = \{u \in \mathbb{F}_2^n \mid a_u = 1\}$. The algebraic degree of g equals r then there exists at least one maximal element $\mathbf{u}$ of Π with respect to the word partial ordering $\preceq$ whose hamming weight equals r. We then deduce the result from Proposition 3.6.8. □

Remark 3.6.10. *Proposition 3.6.8 says that, for every $w \leq r$,*

$$\dim Mul_k(g) - d_{k,1\oplus g} \geq \sum_{i=k-w+1}^{k} \binom{n-w}{i}$$

if the algebraic normal form of g contains a monomial x^ω, with $\mathrm{wt}(\omega) = w$, which is not contained in any another monomial of g. Now, we have $\sum_{i=k-w+1}^{k} \binom{n-w}{i} \geq \sum_{i=k-r+1}^{k} \binom{n-r}{i}$. This follows from the identity $\binom{n-w}{i} = \sum_{p=i-r+w}^{i} \binom{n-r}{p}\binom{r-w}{i-p}$ and the sequence of equalities

$$\begin{aligned}
&\sum_{i=k-w+1}^{k}\binom{n-w}{i}\\
&=\sum_{i=k-w+1}^{k}\sum_{p=i-r+w}^{i}\binom{n-r}{p}\binom{r-w}{i-p}\\
&=\sum_{p=k-r+1}^{k}\binom{n-r}{p}\sum_{i=max(p,k-w+1)}^{min(p-w+r,k)}\binom{r-w}{i-p}\\
&\geq\sum_{p=k-r+1}^{k}\binom{n-r}{p}.
\end{aligned}\tag{3.26}$$

Therefore, the preceding lower bound on $\dim Mul_k(g)-d_{k,1\oplus g}$ *is better than that of Corollary 3.6.9 if we take* $w<r$*. However, it requires more information on the* n*-variable Boolean function* g *than that of Corollary 3.6.9 that simply depends on the algebraic degree of* g*. Now, we shall need a lower bound that does not depend on the* n*-variable Boolean function* g *to get our result. This is the reason why we shall restrict ourselves to use Corollary 3.6.9 rather than Proposition 3.6.8 in the sequel.*

Remark 3.6.11. *The lower bound of Corollary 3.6.9 is achieved by the complements of the indicators of* $(n-r)$*-dimensional affine subspaces of* $\mathbb{F}_2^n$*, that is, whenever* g *is the complement of an* $(n-r)$*-dimensional affine subspace of* $\mathbb{F}_2^n$*, it holds* $\dim Mul_k(g)-d_{k,1\oplus g}=\sum_{i=k-r+1}^{k}\binom{n-r}{i}$*. Indeed, we have that* $d_{k,1\oplus g}=\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k}\binom{n-r}{i}$ *(Proposition 3.6.4) and* $d_{k,g}=\sum_{i=0}^{k-r}\binom{n-r}{i}$ *(Proposition 3.6.6). Therefore, according to Lemma 3.6.5,* $\dim Mul_k(g)=\sum_{i=0}^{k}\binom{n}{i}-d_{k,g}=\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k-r}\binom{n-r}{i}=\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k}\binom{n-r}{i}+\sum_{i=k-r+1}^{k}\binom{n-r}{i}=d_{k,1\oplus g}+\sum_{i=k-r+1}^{k}\binom{n-r}{i}$*.*

However, we do not know whether there exists or not another Boolean functions that achieve the equality $\dim Mul_k(g)-d_{k,1\oplus g}=\sum_{i=k-r+1}^{k}\binom{n-r}{i}$*. The only fact that we are able to say is deduced from the arguments exposed in Remark 3.6.10, that is, if an* n*-variable Boolean function* g *achieves the equality, then all the maximal elements* x^w *in the ANF of* g *are of algebraic degree* r*.*

Lemma 3.6.12. *([193]) Let* g *be an* n*-variable Boolean function of algebraic degree* r*. Let* k *be a positive integer strictly greater than* r*. Then the subspace* $Mul_{k-r}(1\oplus g)$ *is contained in* $An_k(g)$*.*

Proof. Let p be an element of $Mul_{k-r}(1\oplus g)$. Assume that $p=(1\oplus g)q$ where $q\in\mathcal{RM}(k-r,n)$. Now, $\deg(p)\leq\deg(1\oplus g)+\deg(q)\leq r+k-r=k$. Moreover, one has $p(x)=0$ for every $x\in supp(g)$, that is, p is an annihilator of g. Thus, $Mul_{k-r}(1\oplus g)\subset An_k(g)$. □

Remark 3.6.13. *In the particular case where the* n*-variable Boolean function* g *is the complement of the indicator of an* $(n-r)$*-dimensional affine subspace of* $\mathbb{F}_2^n$*, the subspaces* $Mul_{k-r}(1\oplus g)$ *and* $An_k(g)$ *coincide because their dimensions are equal.*

Indeed, note first that $\dim Mul_{k-r}(1\oplus g)=\sum_{i=0}^{k-r}\binom{n}{i}-d_{k-r,1\oplus g}=\sum_{i=0}^{k-r}\binom{n-r}{i}$ *(since* $d_{k-r,1\oplus g}=\sum_{i=0}^{k-r}\binom{n}{i}-\sum_{i=0}^{k-r}\binom{n-r}{i}$ *by virtue of Proposition 3.6.4). On the other hand, Proposition 3.6.6 says that* $d_{k,g}=\sum_{i=0}^{k-r}\binom{n-r}{i}$*. Thus,* $\dim Mul_{k-r}(1\oplus g)=\sum_{i=0}^{k-r}\binom{n-r}{i}=d_{k-r,g}$*.*

3.6.2 A new lower bound on the r-th-order nonlinearity of n-variable Boolean function with respect to their algebraic immunity (improvements in 2007)

In this subsection, we shall see that the dimension of the vector subspace of all annihilators with prescribed algebraic degree of a Boolean function plays also an important role in relation to the r-th order nonlinearity of this Boolean function.

Given an n-variable Boolean function f and a positive integer k, we denote by $\Re_f(k,n)$ the restriction of the generator matrix of the kth-order Reed-Muller code of length 2^n to the support of f, that is, the columns of this matrix correspond to the evaluation of the monomials of algebraic degree at most k on the support of f. This matrix has $\mathrm{wt}(f)$ rows and $\sum_{i=0}^{k}\binom{n}{i}$ columns. The following result will be useful in the sequel.

Proposition 3.6.14. *([193]) An n-variable Boolean function f has no annihilator of algebraic degree at most k if and only if all the matrices $\Re_f(r,n)$, $r \leq k-1$, are of full rank. Moreover, one has, for every positive integer $k \leq n$,*

$$d_{k,f} + rank\left(\Re_f(k,n)\right) = \sum_{i=0}^{k}\binom{n}{i}. \tag{3.27}$$

Proof. We begin with proving the first assertion. We shall prove it by contraposition, that is, we prove that an n-variable Boolean function f admits an annihilator of algebraic degree at most k if and only if the matrix $\Re_f(k,n)$ is singular.

Suppose first that f admits an annihilator of algebraic degree at most k, that is, there exists an n-variable Boolean function $p \in \mathcal{RM}(k,n)$ such that $f(x)p(x) = 0$ for every $x \in \mathbb{F}_2^n$. This is equivalent to say that $p(x) = 0$ for every $x \in supp(f)$ or, in matrix form, that $\Re_f(k,n)A_p = 0$ (where A_p is the column vector whose entries are the coefficients a_v of the ANF of p, that we assume to be $p(x) = \bigoplus_{\mathrm{wt}(v)\leq k} a_v x^v$). Now, the latter equality is equivalent to say that the matrix $\Re_f(k,n)$ is singular.

Conversely, suppose that the matrix $\Re_f(k,n)$ is singular. The columns vectors $(C_v)_{\mathrm{wt}(v)\leq k}$ of $\Re_f(k,n)$ are then linearly dependent, that is, there exists a family $\{a_v,\ \mathrm{wt}(v) \leq k\}$ of elements of $\mathbb{F}_2$ such that $\bigoplus_{\mathrm{wt}(v)\leq k} a_v C_v = 0$. Now, a column C_v is the truth table of the restriction of the monomial x^v to $supp(f)$. Thus, we have $\bigoplus_{\mathrm{wt}(v)\leq k} a_v x^v = 0$ for every $x \in supp(f)$. Let then $p \in \mathcal{RM}(k,n)$ be the n-variable Boolean function whose ANF is $p(x) = \bigoplus_{\mathrm{wt}(v)\leq k} a_v x^v$. The latter equality is hence equivalent to say that the n-variable Boolean function p is an annihilator of f.

Identity (3.27) is obtained by noting that the dimension of the subspace $Mul_k(f)$ and the rank of $\Re_f(k,n)$ are equal. The result follows then from the fact that $\dim Mul_k(f) = \sum_{i=0}^{k}\binom{n}{i} - d_{k,f}$ (Lemma 3.6.5). □

The rth-order nonlinearity of a Boolean function g is the minimum Hamming distance from f to an n-variable Boolean function g of algebraic degree at most r. Our approach is to establish a lower bound on $\mathrm{dist}(f,g)$ holding for every Boolean function g of algebraic degree r. To this end, we first establish a lower bound on $\mathrm{dist}(f,g)$ involving the sum of the two dimensions $d_{k-1,g}$ and $d_{k-1,1\oplus g}$. This is the key result that will enable to improve further the lower bound of [34, 30].

Lemma 3.6.15. *([193]) Let f be an n-variable Boolean function. Suppose that $AI(f) = k$. Let r be a positive integer strictly less than k. Then, for every n-variable Boolean function g of algebraic degree at most r, we have*

$$\mathrm{dist}(f,g) \geq d_{k-1,g} + d_{k-1,1\oplus g}.$$

Proof. Denote by d the number of bits to be modified in the truth table of f to obtain g. Denote by d_i, $i \in \{0,1\}$, the number of words of $supp(i \oplus f)$ for which we modify the output value of $i \oplus f$. Clearly, we have $\mathrm{dist}(f,g) = d = d_0 + d_1$.

Now, for every positive integer ℓ, The matrix $\Re_g(\ell, n)$ is deduced from the matrix $\Re_f(\ell, n)$ by deleting d_0 rows and adding d_1 rows. The matrix $\Re_f(k-1, n)$ being of full rank according to proposition 3.6.14, we hence have that $rank(\Re_g(k-1,n)) \geq \sum_{i=0}^{k-1} \binom{n}{i} - d_0$ and thus that $d_0 \geq \sum_{i=0}^{k-1} \binom{n}{i} - rank(\Re_g(k-1,n)) = d_{k-1,g}$.

Similarly, the matrix $\Re_{1\oplus g}(\ell, n)$ is deduced from the matrix $\Re_{1\oplus f}(\ell, n)$ by deleting d_1 rows and adding d_0 rows. The matrix $\Re_f(k-1, n)$ being also of full rank, we hence deduce by similar arguments as those exposed previously that $d_1 \geq d_{k-1,1\oplus g}$. □

Remark 3.6.16. *Collecting together Lemma 3.6.6 applied to affine Boolean functions and Lemma 3.6.15 leads to* $\mathrm{dist}(f,l) \geq d_{k-1,l} + d_{k-1,1\oplus l} = 2\sum_{i=0}^{k-2} \binom{n-1}{i}$ *for every n-variable affine Boolean functions, that is, we recover the lower bound of [171].*

Similarly, applying Lemma 3.6.15 to n-variable Boolean functions of algebraic degree at most r leads to $\mathrm{dist}(f,g) \geq 2\sum_{i=0}^{k-r-1} \binom{n-r}{i}$*, that is, we recover the first lower bound of [30, Theorem 1].*

We then deduce from Lemma 3.6.8 and Lemma 3.6.15 our lower bound on the rth-order linearity of an n-variable Boolean function with prescribed algebraic immunity. Our idea is to get a lower bound on this sum rather than considering separately the two dimensions $d_{k-1,g}$ and $d_{k-1,1\oplus g}$.

Theorem 3.6.17. *([193]) Let f be an n-variable Boolean function of algebraic immunity k and let r be a positive integer strictly less than k. Then*

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$$

Proof. Let g be an arbitrary n-variable Boolean function of algebraic degree at most r. According to Lemma 3.6.15, we have

$$\mathrm{dist}(f,g) \geq d_{k-1,g} + d_{k-1,1\oplus g}.$$

Now, according to Lemma 3.6.12, one has $An_{k-1}(g \oplus 1) \supset Mul_{k-r-1}(g)$ and $An_{k-1}(g) \supset Mul_{k-r-1}(1 \oplus g)$. Hence

$$\begin{aligned}\mathrm{dist}(f,g) \geq d_{k-1,g} + d_{k-1,1\oplus g} &\geq \dim Mul_{k-r-1}(g) \\ &\quad + \dim Mul_{k-r-1}(1 \oplus g)\end{aligned}$$

Next, thanks to Lemma 3.6.5, we get

$$\begin{aligned}\mathrm{dist}(f,g) &\geq \dim Mul_{k-r-1}(g) + \dim Mul_{k-r-1}(1 \oplus g) \\ &= \sum_{i=0}^{k-r-1} \binom{n}{i} + \dim Mul_{k-r-1}(g) - d_{k-r-1,1\oplus g}.\end{aligned}$$

We finally conclude thanks to Corollary 3.6.9 that says that $\dim Mul_{k-r-1}(g) - d_{k-r-1,1\oplus g} \geq \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$. □

n \ r	2	3	4	5	6	7
18	**43556**	**17439**	**5518**	1976	344	38
19	**126008**	**57992**	**21592**	**6507**	2320	382
20	**188368**	**81404**	**28568**	8826	2702	422
21	**527900**	**257396**	**103784**	**34780**	15094	3124
22	**803860**	**369748**	**141064**	**44844**	18218	3588
23	**2195580**	**1123220**	**483680**	**176660**	**53954**	21806
24	**3396320**	**1645660**	**672784**	**233827**	**68071**	25902
25	**9080772**	**4838490**	**2202164**	**863975**	**289301**	136812
26	**14239032**	**7211198**	**3125248**	**1169920**	**374371**	167364
27	**37392864**	**20633040**	**9846132**	**4104275**	**1484042**	**458054**
28	**59333408**	**31214643**	**14221898**	**5670245**	**1963795**	**581338**
29	**153434536**	**87279291**	**43393566**	**19055725**	**7355234**	**2462995**
30	**246025562**	**133797407**	**63665462**	**26799567**	**9928262**	**3194667**

Table 3.1 – Best lower bounds on $nl_r(f)$ for $18 \leq n \leq 30$, $AI(f) = \lceil \frac{n}{2} \rceil$, $r \leq 7$

Remark 3.6.18. *In the particular case where $r = 1$, Theorem 3.6.17 says that $nl(f) \geq \sum_{i=0}^{k-2} \binom{n}{i} + \binom{n-1}{k-2}$. Now, note that, using the identity $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$, we have $\sum_{i=0}^{k-2} \binom{n}{i} = 1 + \sum_{i=1}^{k-2} \binom{n-1}{i} + \sum_{i=1}^{k-2} \binom{n-1}{i-1} = 2\sum_{i=0}^{k-3} \binom{n-1}{i} + \binom{n-1}{k-2}$. Thus, we get $nl(f) \geq 2\sum_{i=0}^{k-2} \binom{n-1}{i}$ which is exactly the lower bound of [171].*

Remark 3.6.19. *Theorem 3.6.17 improves further the result of [34] for all orders. We present in Table 9.4 the comparison between our lower bound and the lower bound of [34]. On the other hand, it only improves partially the result of [30]. We present in table 3.2 the comparison between the lower bound of Theorem 3.6.17 and the lower bound of [30]. Moreover, we give in table 3.1 the best lower bound between ours (that we write in bold text) and those of [30]. We have checked by computer experiments that, for every $n \leq 60$, our lower bound improves the lower bound of [30] for $2 \leq k \leq \lceil \frac{n}{2} \rceil$ and $2 \leq r \leq \lfloor \frac{k-1}{2} \rfloor$ while it does not improve the lower bound of [30] for $2 \leq k \leq \lceil \frac{n}{2} \rceil$ and $\lfloor \frac{k-1}{2} \rfloor + 3 \leq r \leq k$. However, we do not know whether it holds for every positive integer n or not. Concerning the cases where $r \in \left\{ \lfloor \frac{k-1}{2} \rfloor + 1, \lfloor \frac{k-1}{2} \rfloor + 2 \right\}$, we have found by computer experiments that our lower bound is better than the lower bound of [30] for some values of (k, n) with $n \leq 60$ and $2 \leq k \leq \lceil \frac{n}{2} \rceil$.*

3.7 Recent constructions of Boolean functions satisfying the main cryptographic criteria

Building a Boolean function meeting as many criteria as possible is a difficult task. Trade-offs must usually be made between them. Since the introduction of algebraic immunity, several constructions of Boolean functions with high algebraic immunity have been suggested, but very few of them are of optimal algebraic immunity. More importantly, those having other good cryptographic properties, as balancedness or high nonlinearity for instance, are even rarer. Among those having optimal algebraic immunity $AI(f) = \lceil n/2 \rceil$, most have a poor nonlinearity [49, 78, 164, 165, 51], close to the lower bound of Lobanov [172]:

$$\mathrm{nl}(f) \geq 2^{n-1} - \binom{n}{\lfloor \frac{n}{2} \rfloor} .$$

n \ r	2	3	4	5	6	7
18	1.46	1.76	1.88	0.69	0.73	0.82
19	1.53	1.95	2.18	1.01	0.66	0.71
20	1.49	1.87	2.07	0.92	0.67	0.72
21	1.55	2.04	2.38	2.30	0.63	0.65
22	1.52	1.96	2.26	2.38	0.64	0.66
23	1.58	2.13	2.57	2.83	1.33	0.62
24	1.55	2.05	2.44	2.67	1.21	0.62
25	1.60	2.20	2.74	3.13	2.11	0.59
26	1.57	2.12	2.60	2.95	2.24	0.60
27	1.61	2.27	2.90	3.42	3.74	1.77
28	1.59	2.19	2.76	3.22	3.50	1.60
29	1.63	2.33	3.05	3.69	4.17	2.12
30	1.60	2.26	2.90	3.48	3.90	2.08

Table 3.2 – The new lower bound over the lower bound of [30] for $18 \leq n \leq 30$, $AI(f) = \left\lceil \frac{n}{2} \right\rceil$, $r \leq 7$

n \ r	2	3	4	5	6	7
18	1.40	1.38	1.36	1.38	1.46	1.63
19	1.34	1.32	1.30	1.29	1.33	1.41
20	1.37	1.35	1.32	1.31	1.35	1.44
21	1.31	1.30	1.26	1.25	1.26	1.30
22	1.34	1.32	1.28	1.27	1.28	1.32
23	1.29	1.27	1.24	1.21	1.21	1.23
24	1.32	1.29	1.25	1.23	1.23	1.25
25	1.28	1.26	1.22	1.19	1.18	1.18
26	1.30	1.27	1.23	1.20	1.19	1.20
27	1.26	1.24	1.20	1.17	1.15	1.15
28	1.28	1.26	1.22	1.18	1.17	1.16
29	1.25	1.23	1.19	1.16	1.14	1.13
30	1.27	1.24	1.20	1.17	1.15	1.14

Table 3.3 – The new lower bound over the lower bound of [34] for $18 \leq n \leq 30$, $AI(f) = \left\lceil \frac{n}{2} \right\rceil$, $r \leq 7$

We now present different *good* families, i.e. meeting most of the criteria mentioned in Section 3.2 in a satisfactory way.

In 2008, Carlet and Feng [50] studied a family of Boolean functions introduced by Feng, Liao and Yang [100] and devised the first infinite class of functions which seems able to satisfy all of the main criteria for being used as a filtering function in a stream cipher.

Definition 3.7.1 (Construction of Carlet and Feng [50, Section 3]). *Let $n \geq 2$ be a positive integer and α a primitive element of $\mathbb{F}_{2^n}$. Let f be the Boolean function in n variables defined by*

$$\mathrm{supp}(f) = \left\{0, 1, \alpha, \ldots, \alpha^{2^{n-1}-2}\right\} \ .$$

They proved that these functions are

1. balanced,
2. of optimal algebraic degree $n-1$ for a balanced function,
3. of optimal algebraic immunity $\lceil n/2 \rceil$,
4. with good immunity to fast algebraic attacks,
5. and with good nonlinearity

$$\mathrm{nl}(f) \geq 2^{n-1} + \frac{2^{n/2+1}}{\pi} \ln\left(\frac{\pi}{2^n - 1}\right) - 1 \approx 2^{n-1} - \frac{2\ln 2}{\pi} n 2^{n/2} \ .$$

Moreover, it was checked for small values of n that the functions had far better nonlinearity than the proved lower bound.

Afterwards, the same family was reintroduced in a different way by Wang et al. [260, 48] who proved a better lower bound:

$$\mathrm{nl}(f) \geq \max\left(6\lfloor\frac{2^{n-1}}{2n}\rfloor - 2, 2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{3}{2}\right) 2^{n/2}\right) \ .$$

Finally, Tang, Carlet and Tang [245] proved in 2011 that the following better lower bound is again valid:

$$\mathrm{nl}(f) \geq 2^{n-1} - \left(\frac{n\ln 2}{2\pi} + 0.74\right) 2^{n/2} - 1 \ .$$

In 2010, Tu and Deng [249] discovered that there may be Boolean functions of optimal algebraic immunity in a classical class of Partial Spread functions due to Dillon [86] provided that the following combinatorial conjecture is correct.

Conjecture 3.7.2 (Tu–Deng conjecture). *For all $k \geq 2$ and all $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | a + b = t \text{ and } w_2(a) + w_2(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

Tu and Deng checked the validity of the conjecture for $k \leq 29$. They also proved that, if the conjecture is true, then one can get in even dimension balanced Boolean functions of optimal algebraic immunity and of high nonlinearity (better than that of the functions described above proposed by Carlet and Feng.

More explicitly, their idea was to apply the idea of Carlet and Feng to the classical construction of Dillon ([82]); more precisely, functions form the so-called Partial Spread class $\mathcal{PS}_{ap}$ (see in

Subsection 4.4.1) whose elements are defined in an explicit form: $f(x,y) = g(\frac{x}{y})$ (*i.e.* $g(xy^{2^k-2})$) with $\frac{x}{y} = 0$ if $y = 0$ where f is a Boolean function defined on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and g be a balanced Boolean function defined over $\mathbb{F}_{2^k}$ such that $g(0) = 0$. Functions in the class $\mathcal{PS}_{ap}$ are bent and have algebraic degree $n/2 = k$ ([227]).

Definition 3.7.3 (First construction of Tu and Deng [249])**.** *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ a Boolean function in k variables defined by*

$$\begin{aligned}\mathrm{supp}(g) &= \left\{\alpha^s, \alpha^{s+1}, \ldots, \alpha^{s+2^{k-1}-1}\right\} \\ &= \alpha^s A \ ,\end{aligned}$$

for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by

$$f(x,y) = \begin{cases} g\left(\frac{x}{y}\right) & \text{if } x \neq 0 \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

They proved that these functions are

1. bent (because they belong to $\mathcal{PS}_{ap}$),
2. of algebraic degree $n/2 = k$ [228],
3. and of optimal algebraic immunity $n/2 = k$ if Conjecture 3.7.2 is verified.

To prove the optimal algebraic immunity, Tu and Deng have adopted to their function the approach of Carlet and Feng which consists to identify annihilators of the Boolean function with codewords of BCH codes [175, 176, 252]. The role of the conjecture is then to deduce from the BCH bound [175, 176, 252] that those codewords are equal to zero if the algebraic degrees of the corresponding annihilators are less than $n/2 = k$.

These functions can then be modified to give rise to functions with different good cryptographic properties as follows.

Definition 3.7.4 (Second construction of Tu and Deng [249])**.** *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ a Boolean function in k variables defined by*

$$\mathrm{supp}(g) = \alpha^s A \ ,$$

for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by

$$f(x,y) = \begin{cases} g\left(\frac{x}{y}\right) & \text{if } xy \neq 0 \ , \\ 1 & \text{if } x = 0 \text{ and } y \in (\alpha A)^{-1} \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

Our definition slightly differs from the original one [249], but, in the end, it is equivalent because

$$\begin{aligned}(\alpha A)^{-1} &= \left\{\alpha^{-1}, \ldots, \alpha^{-(2^{k-1}-1)}, \alpha^{-2^{k-1}}\right\} \\ &= \left\{\alpha^{2^{k-1}-1}, \alpha^{2^{k-1}}, \ldots, \alpha^{2^k-2}\right\} \ .\end{aligned}$$

The cryptographic parameters of the function f are as follows:

1. f is balanced;
2. its algebraic degree is optimal for a balanced function, that is equal to $n-1$;
3. up to Conjecture 3.7.2, f has optimal algebraic immunity that is, $AI(f) = n$;
4. its nonlinearity satisfies

$$\mathrm{nl}(f) \geq 2^{n-1} - 2^{n/2-1} - \frac{n}{2} 2^{n/4} \ln 2 - 1 \ .$$

Afterwards, Tu and Deng [248, 247] modified their original functions to obtain a class of 1-resilient functions with high nonlinearity and high algebraic immunity.

Definition 3.7.5 (Third construction of Tu and Deng [248, 247])**.** *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\right\}$, $0 \leq s \leq 2^k - 2$ an integer and $B = \{0,1\} \cup A^{-1}$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by*

$$\mathrm{supp}(f) = \bigcup \begin{cases} \{(x,y) \mid x/y \in \alpha^s A\} \ , \\ \{(x,y) \mid y = \alpha^{-s} y, x \in B\} \ , \\ \{(x,0) \mid x \in \mathbb{F}_{2^k} \setminus B\} \ , \\ \{(0,y) \mid y \in \mathbb{F}_{2^k} \setminus \alpha^{-s} B\} \ . \end{cases}$$

They proved that f satisfies the following properties:

1. f is 1-resilient;
2. f is of optimal algebraic degree $\deg(f) = n-2$;
3. up to Conjecture 3.7.2, f has algebraic immunity $AI(f) \geq n/2 - 1$;
4. f has nonlinearity

$$\mathrm{nl}(f) \geq 2^{n-1} - 2^{n/2-1} - \frac{3}{2} n 2^{n/4} \ln 2 - 7 \ .$$

It is in fact proved that f has optimal algebraic immunity depending only on Conjecture 3.7.2 when $n/2$ is odd and on an additional assumption when $n/2$ is even [247].

Finally, Tang et al. [246] applied a degree optimized version of an iterative construction of balanced Boolean functions with very high nonlinearity by Dobbertin [94] to the functions constructed by Tu and Deng [249, 248] and obtained functions with better nonlinearity. For $n = 2k = 2^t m \geq 4$, m odd, their first family is

1. balanced,
2. of optimal algebraic degree $n-1$,
3. of optimal algebraic immunity $n/2$ if Conjecture 3.7.2 is verified,
4. of nonlinearity at least

$$2^{n-1} - \sum_{i=0}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m-1)/2} \ ;$$

and their second family is

1. 1-resilient,

2. of optimal algebraic degree $n-2$,

3. of algebraic immunity at least $n/2-1$ if Conjecture 3.7.2 is verified,

4. of nonlinearity at least

$$\begin{cases} 2^{n-1} - 2^{n/2-1} - 3\left(\sum_{i=1}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m-1)/2}\right) & \text{if } m = 1 \ , \\ 2^{n-1} - 2^{n/2-1} - 3\sum_{i=1}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m+1)/2} - 6 & \text{if } m \geq 2 \ . \end{cases}$$

Unfortunately, Carlet [47] observed that the functions introduced by Tu and Deng are weak against fast algebraic attacks and unsuccessfully tried to repair their weakness. It was subsequently shown by Wang and Johansson [259] that this family can not be easily repaired.

Nonetheless, more recent developments have shown that the construction of Tu and Deng and the associated conjecture are not of purely æsthetic interest, but are interesting tools in a cryptographic context.

In 2011, inspired by the previous work of Tu and Deng [249], Tang, Carlet and Tang [245] constructed an infinite family of Boolean functions with many good cryptographic properties. The main idea of their construction is to change the division in the construction of Tu and Deng by a multiplication. The associated combinatorial conjecture is then modified as follows.

Conjecture 3.7.6 (Tang–Carlet–Tang conjecture)**.** *For all $k \geq 2$ and all $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid a - b = t; w_2(a) + w_2(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

They verified it experimentally for $k \leq 29$, as well as the following generalized property for $k \leq 15$ where $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ is such that $\gcd(u, 2^k-1) = 1$ and $\epsilon = \pm 1$.

Conjecture 3.7.7 (Tang–Carlet–Tang conjecture)**.** *Let $k \geq 2$ be an integer, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ such that $\gcd(u, 2^k-1) = 1$ and $\epsilon \in \{-1, 1\}$. Then*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua + \epsilon b = t; w_2(a) + w_2(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

This generalized conjecture includes the original conjecture proposed by Tu and Deng (Conjecture 3.7.2) for $u = 1$ and $\epsilon = +1$.

The construction of their functions is as follows.

Definition 3.7.8 (Construction of Tang, Carlet and Tang [245])**.** *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ the Boolean function in k variables defined by*

$$\mathrm{supp}(g) = \alpha^s A \ ,$$

for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by

$$f(x,y) = g\left(xy\right) \ .$$

They proved that such a function f is

1. of algebraic degree $n-2$,

2. of optimal algebraic immunity $n/2$ if Conjecture 3.7.6 is true,

3. of good immunity against fast algebraic attacks,

4. of nonlinearity at least
$$2^{n-1} - \left(\frac{\ln 2}{2\pi} n + 0.42\right) 2^{n/2} - 1 \ .$$

The proof of the optimality of the algebraic immunity is similar to the proof of Tu and Deng [249].

These functions can then be modified using the same procedure as Tang et al. [246] to obtain balanced functions with high algebraic degree and nonlinearity. They proved that, for $n = 2k = 2^t m \geq 4$ and m odd, these modified functions are

1. balanced,

2. of optimal algebraic degree $n-1$,

3. of optimal algebraic immunity $n/2$ if Conjecture 3.7.6 is true,

4. of good immunity against fast algebraic attacks,

5. of nonlinearity at least
$$\begin{cases} 2^{n-1} - \left(\frac{\ln 2}{2\pi} n + 0.42\right) 2^{n/2} - 2^{\frac{n/2-1}{2}} - 1 & \text{if } t = 1 \ , \\ 2^{n-1} - \left(\frac{\ln 2}{2\pi} n + 0.42\right) 2^{n/2} - \sum_{i=1}^{t-1} 2^{n/(2^{i+1})-1} - 2^{(m-1)/2} - 1 & \text{if } t \geq 2 \ . \end{cases}$$

It should finally be mentioned that Jin et al. [139] generalized the construction of Tang, Carlet and Tang [245] in a way that included back the construction of Tu and Deng [249]. In their paper, the main idea is to replace y by y^{2^k-1-u} in the construction of the function. Hence, the family of Tu and Deng is included for $u = 1$, and the family of Tang et al. for $u = 2^k - 2$. The associated combinatorial conjecture is then modified as follows.

Conjecture 3.7.9 (Jin et al. conjecture)**.** *Let $k \geq 2$ be an integer, $t, u, v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ such that $\gcd(u, 2^k-1) = \gcd(v, 2^k-1) = 1$. Then*
$$\# \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua + vb = t; w_2(a) + w_2(b) \leq k-1 \right\} \leq 2^{k-1} \ .$$

This generalized conjecture obviously includes all the previous ones.

The construction of their functions is as follows.

Definition 3.7.10 (Construction of Jin et al. [139])**.** *Let $n = 2k \geq 4$ be an even integer, α a primitive element of $\mathbb{F}_{2^n}$, $A = \left\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\right\}$ and $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ Boolean function in k variables defined by*
$$\mathrm{supp}(g) = \alpha^s A \ ,$$
for any $0 \leq s \leq 2^k - 2$. Let $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be the Boolean function in n variables defined by
$$f(x,y) = g\left(xy^{2^k-1-u}\right) \ .$$

They proved that such a function f is

1. of algebraic degree between $n/2$ and $n-2$ depending on the value of u,

2. of optimal algebraic immunity $n/2$ if Conjecture 3.7.9 is true,

3. of nonlinearity at least

$$2^{n-1} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/2} - 1 \approx 2^{n-1} - \frac{\ln 2}{\pi} n 2^{n/2} \ .$$

The proof of the optimality of the algebraic immunity is once again similar to the previous ones. It should be noted that resistance to fast algebraic attacks is not studied by Jin et al. [139].

Modifying these functions as before, Jin et al. obtained balanced functions with high algebraic degree and nonlinearity. They proved that for $n = 2k \geq 4$, these modified functions are

1. balanced,
2. of optimal algebraic degree $n-1$,
3. of optimal algebraic immunity $n/2$ if Conjecture 3.7.9 is true,
4. of nonlinearity at least

$$2^{n-1} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/2} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/4} - 2 \approx 2^{n-1} - \frac{\ln 2}{\pi} n 2^{n/2} - \frac{\ln 2}{\pi} n 2^{n/4} \ .$$

Jin et al. [138] applied a similar generalization to the 1-resilient Boolean function of Tu and Deng [247] and obtained a family functions which are

1. 1-resilient,
2. of optimal algebraic degree $n-2$,
3. of optimal algebraic immunity $n/2$ up to Conjecture 3.7.9 and an additional assumption,
4. of nonlinearity at least

$$\begin{aligned} &2^{n-1} - \frac{2}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/2} - 2^{n/2-1} - \frac{4}{\pi} \ln \frac{4(2^{n/2}-1)}{\pi} 2^{n/4} - 3 \\ &\approx 2^{n-1} - \frac{\ln 2}{\pi}(n+1) 2^{n/2} - \frac{2 \ln 2}{\pi} n 2^{n/4} \ . \end{aligned}$$

3.8 Some results on a conjecture about binary strings distribution

As was underlined in the previous section , the good cryptographic properties of the Boolean functions of the Jin et al. family [138] and more precisely the optimality of their algebraic immunity, depend on the validity of a combinatorial conjecture. The purpose of this section, if not to prove that conjecture in its full generality, is at least to give a good insight into its expected validity not only through a thorough theoretical study.

.

Unless stated otherwise, we use the following notation throughout this section:

- $k \in \mathbb{N}$ is the number of bits (or length of binary strings) we are currently working on;
- $t \in \mathbb{Z}/(2^k - 1)\mathbb{Z}$ is a fixed modular integer.

We use the following function of natural (or modular) integers (or binary strings).

Let us denote by $S_{t,v,u,k}$ the set of interest:

$$S_{t,v,u,k} = \left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua + vb = t; w_2(a) + w_2(b) \leq k-1\right\} \ ,$$

where $k \geq 2$, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ and $u, v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^\times$, i.e. u and v are invertible modulo 2^k-1.

We now recall the different flavors of the conjecture already mentioned in the previous section.

Conjecture 3.7.2 (Tu–Deng conjecture)**.** *With the above notation,*

$$\#S_{t,+1,1,k} \leq 2^{k-1} \ .$$

Conjecture 3.7.6 (Tang–Carlet–Tang conjecture)**.** *With the above notation,*

$$\#S_{t,-1,1,k} \leq 2^{k-1} \ .$$

Conjecture 3.7.9 (Jin et al. conjecture)**.** *With the above notation,*

$$\#S_{t,v,u,k} \leq 2^{k-1} \ .$$

In the following, we present first general basic properties of the set $S_{t,v,u,k}$ obtained by studying the behavior of the Hamming weight under various basic transformations: *binary not* and *rotation*. In fact, in 2010, we have studied these properties in the particular case of $S_{t,+1,1,k}$ (that we denoted simply by $S_{t,k}$) since the other conjectures were formulated only in 2011. For making the paper self-contained, we include the results formulated by Flori and Randriam [106] in the general case.

Definition 3.8.1. *We define $\overline{a}^k$ as the modular integer whose binary expansion is the binary not on k bits of the binary expansion of the representative of a in $\{0, \ldots, 2^k-2\}$. We denote it by $\overline{a}$ when there is no ambiguity about the value of k.*

Lemma 3.8.2. *[105] Let $a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ be a non-zero modular integer, then $-a = \overline{a}$ and $w_2(-a) = k - w_2(a)$.*

Proof. Indeed $a + \overline{a} = \sum_{i=0}^{k-1} 2^i = 2^k - 1 = 0$. □

Lemma 3.8.3. *[105] For all $i \in \mathbb{Z}$ and $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, we have*

$$w_2(2^i a) = w_2(a) \ .$$

Proof. We are working in $\mathbb{Z}/(2^k-1)\mathbb{Z}$ so that $2^k = 1$ and multiplying a modular integer in $\mathbb{Z}/(2^k-1)\mathbb{Z}$ by 2 is just rotating its representation as a binary string on k bits by one bit to the left, whence the equality of the Hamming weights. □

Therefore, we say that, for any $i \in \mathbb{Z}$, $2^i a$ and a are equivalent, or that they are in the same *cyclotomic class* modulo 2^k-1, and we write $a \simeq 2^i a$. Remark that, for a given $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, b must be equal to $v^{-1}(t-ua)$, whence the following lemma.

Lemma 3.8.4. *[105] For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2(v^{-1}(t-ua)) \leq k-1\right\} \ .$$

Using the previous lemmas, we can now show that is enough to study the conjecture for one t, but also one u and one v, in each cyclotomic class.

Lemma 3.8.5. *[105] For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{2t,v,u,k} \ .$$

Proof. Indeed $a \mapsto 2a$ is a permutation of $\mathbb{Z}/(2^k-1)\mathbb{Z}$ so that

$$\begin{aligned}
\#S_{2t,v,u,k} &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2(v^{-1}(2t-ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(2a) + w_2(2v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#S_{t,v,u,k} \ .
\end{aligned}$$

□

Lemma 3.8.6. *[105] For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{t,v,2u,k} \ .$$

Proof. Using the previous lemma,

$$\begin{aligned}
\#S_{t,v,2u,k} &= \#S_{2t,v,2u,k} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2(v^{-1}(2t-2ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#S_{t,v,u,k} \ .
\end{aligned}$$

□

Lemma 3.8.7. *[105] For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{t,2v,u,k} \ .$$

Proof. Using the previous lemmas,

$$\begin{aligned}
\#S_{t,2v,u,k} &= \#S_{2t,2v,2u,k} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2((2v)^{-1}(2t-2ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#S_{t,v,u,k} \ .
\end{aligned}$$

□

It was shown a more elaborate relation for different values of u, v and t.

Lemma 3.8.8. *[105] For $k \geq 2$,*

$$\#S_{t,v,u,k} = \#S_{(uv)^{-1}t,v^{-1},u^{-1},k} \ .$$

Proof. We use the fact that $a \mapsto u^{-1}(-va+t)$ is a permutation of $\mathbb{Z}/(2^k-1)\mathbb{Z}$ and deduce

$$\begin{aligned}
\#S_{t,v,u,k} &= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(a) + w_2(v^{-1}(t-ua)) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(u^{-1}(-va+t)) + w_2(a) \leq k-1\right\} \\
&= \#\left\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid w_2(v((uv)^{-1}t - u^{-1}a)) + w_2(a) \leq k-1\right\} \\
&= \#S_{(uv)^{-1}t,v^{-1},u^{-1},k} \ .
\end{aligned}$$

□

Now, we state the following observation of Jin et al. [139].

Lemma 3.8.9. *For $k \geq 2$ and $c \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^\times$,*

$$\#S_{t,v,u,k} = \#S_{ct,cv,cu,k} \ .$$

Proof. Indeed, we have $ua + vb = t$ if and only if $cua + cvb = ct$ when c is invertible, whence a bijection between the sets $S_{t,v,u,k}$ and $S_{ct,cv,cu,k}$. □

Finally, as noted by Jin et al. [139], their generalized conjecture is then equivalent to the generalized conjecture of Tang et al. [245].

Now, we concentrate our efforts on the original conjecture of Tu and Deng [249] which is a natural candidate to extend the study of the other conjectures but also because we have interested on this conjecture in 2010 while the other conjectures have been reformulated only in 2011.

In the following, we just give some results appeared in [104][6]. Readers interested in the development of this study will refer to the work of Flori and Randriam [106].

Our main approach used in this section is that of reformulating the conjecture in terms of *carries* occurring in an addition modulo $2^k - 1$. Although such an approach may at first seem quite naive to the reader, what makes the study of the conjecture seemingly so difficult is precisely that a suitable algebraic structure to cast upon the problem has yet to be found, so that only a purely combinatorial point of view is possible as of today.

Let us define the main tool we will use to study the conjecture of Tu and Deng (as well as the other conjectures[7]).

Definition 3.8.10. *For $a \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, we set*

$$r(a,t) = w_2(a) + w_2(t) - w_2(a+t) \ ,$$

i.e. $r(a,t)$ is the number of carries occurring while performing the addition. By convention, we set

$$r(0,t) = k \ ,$$

i.e. 0 behaves like the $\underbrace{\texttt{1...1}}_{k}$ binary string. We also remark that $r(-t,t) = k$.

The following statement is fundamental. It brings to light the importance of the number of carries occurring during the addition.

Proposition 3.8.11. *[104] For $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#S_{t,k} = \#\left\{a \mid r(a,t) > w_2(t)\right\} \ .$$

Now, we often compute $P_{t,k} = 2^{-k}\#S_{t,k}$ rather than $\#S_{t,k}$. Therefore we use the words *proportion* or *probability* in place of *cardinality*. Moreover we often computed cardinalities considering all the binary strings on k bits, i.e. including `1...1` and `0...0`. The modular integer 0 is considered to act as the binary string `1...1` , but the binary string `0...0` should be discarded when doing final computation of $P_{t,k}$. However it ensures that variables are truly *independent*.

The original conjecture proposed by Tu and Deng [249] can be reformulated as follows.

[6] Note that the author had contributed in a smallest part of the joint work with Jean-Pierre Flori, Gérard Cohen and Hugues Randriam. For more details, the reader may refer to [104]. Moreover, Jean-Pierre Flori had continued to study more deeply this conjecture in his PhD thesis [105] and obtained different interesting results, but unfortunately without reaching a complete proof of this conjecture.

[7] Note that Cohen and Flori [67] have used this tool to prove the Conjecture of Tang et al.

Conjecture 3.7.2. *For $k \geq 2$ and $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, let $S_{t,k}$ be the following set*[8]*. :*

$$S_{t,k} = \left\{ a \in \mathbb{Z}/(2^k-1)\mathbb{Z} \mid r(a,t) > w_2(t) \right\} \ ,$$

and $P_{t,k}$ the fraction[9] *of modular integers in $S_{t,k}$:*

$$P_{t,k} = \#S_{t,k}/2^k \ .$$

Then

$$P_{t,k} \leq \frac{1}{2} \ .$$

Tu and Deng verified computationally the validity of this assumption for $k \leq 29$ in about fifteen days on a quite recent computer [249]. We also implemented their algorithm and were able to check the conjecture for $k = 39$ in about twelve hours and fifteen minutes on a pool of about four hundred quite recent cores, and $k = 40$ on a subset of these computers. The algorithm of Tu and Deng [249, Appendix] as well as the implementation have been described by Flori.

Note that conjecture is not only interesting in a cryptographic context, but also for purely arithmetical reasons. For a fixed modular integer $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, it is indeed natural to expect the number of carries occurring when adding a random modular integer $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ to t to be roughly the Hamming weight of t. Note that following this idea, Flori and Randriam [106] have studied the distribution of the number of carries around this value and proved that quite unexpectedly, the conjecture seems to indicate a kind of regularity.

Proposition 3.8.11 allows us to prove the conjecture in the specific case where $t \simeq -t$:

Theorem 3.8.12. *([104]) If $t \simeq -t$, then $\#S_{t,k} \leq 2^{k-1}$.*

Next, we split $t(\neq 0)$ (once correctly rotated, i.e. we multiply it by a correct power of 2 so that its binary expansion on k bits begins with a `1` and ends with a `0`) in blocks of the form $[1^*0^*]$ (i.e. as many `1`s as possible followed by as many `0`s as possible).

Definition 3.8.13. *We denote the number of blocks by d and the numbers of `1`s and `0`s of the ith block t_i by α_i and β_i.*

We have defined corresponding variables for a (a number to be added to t): γ_i the number of `0`s in front of the end of the `1`s subblock of t_i, δ_i the number of `1`s in front of the end of the `0`s subblock of t_i.

Those definitions are depicted below:

$$t = \overbrace{\texttt{1---1}}^{\alpha_1}\overbrace{\texttt{0---0}}^{\beta_1}\texttt{...}\overbrace{\texttt{1---1}}^{\alpha_i}\overbrace{\texttt{0---0}}^{\beta_i}\texttt{...}\overbrace{\texttt{1---1}}^{\alpha_d}\overbrace{\texttt{0---0}}^{\beta_d} \ ,$$
$$a = \texttt{?}\underbrace{\texttt{10-0}}_{\gamma_1}\texttt{?}\underbrace{\texttt{01-1}}_{\delta_1}\texttt{...?}\underbrace{\texttt{10-0}}_{\gamma_i}\texttt{?}\underbrace{\texttt{01-1}}_{\delta_i}\texttt{...?}\underbrace{\texttt{10-0}}_{\gamma_d}\texttt{?}\underbrace{\texttt{01-1}}_{\delta_d} \ ,$$

One should be aware that γ_is and δ_is depend on a and are considered as variables.

We first "approximate" the number of carries $r(a,t)$ by $\sum_{i=0}^{d} \alpha_i - \gamma_i + \delta_i$ ignoring the two following facts:

[8] It is easy to see that this formulation is equivalent to the original one. A formal proof will be given in Corollary 3.8.11

[9] We are fully aware that there are only $2^k - 1$ elements in $\mathbb{Z}/(2^k-1)\mathbb{Z}$, but we will often use the abuse of terminology we make here and speak of *fraction*, *probability* or *proportion* for $P_{t,k}$.

- if a carry goes out of the $i-1$st block (we say that it *overflows*) and $\delta_i = \beta_i$, the 1s subblock produces α_i carries, whatever value γ_i takes,
- and if no carry goes out of the $i-1$st block (we say that it is *inert*), the 0s subblock produces no carry, whatever value β_i takes.

Our first result is the exact formulas of $\#S_{t,k}$ for numbers made of only one block (i.e for $d = 1$). More precisely, we have proved the following theorem.

Theorem 3.8.14. *([104])*

$$P_{t,k} = \begin{cases} 2^{-\alpha-\beta}\frac{1-2^{-2\alpha}}{3} & \text{if } 1 \leq \alpha \leq \frac{k-1}{2} \\ \frac{1+2^{-2\beta+1}}{3} & \text{if } \frac{k-1}{2} \leq \alpha \leq k-1 \end{cases} .$$

For $\alpha = 1$, it reads $S_{1,k} = 2^{k-2} + 1$ and for $\alpha = k-1$, it reads $S_{-1,k} = 2^{k-1}$.
Next, we introduce the following constraint which greatly simplifies calculations:

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d} \beta_i - 1 = k - w_2(t) - 1 \ .$$

That condition tells us that, if a is in $S_{t,k}$, a carry has to go through each subblock of 1s Moreover, it leads us to a proof that the conjecture is *asymptotically* (that is, when $\beta_i \to \infty$) true. More precisely, we have proved the following theorem.

Theorem 3.8.15. *([104]) Let d be a strictly positive integer. There exists a constant K_d such that if t verifies the two following constraints:*

$$\forall i, \beta_i \geq K_d \text{ and } \min_i \alpha_i \geq k - w_2(t) - 1 \ ,$$

then $\#S_{t,k} < 2^{k-1}$.

When the number of blocks, d, goes as well to infinity, we remark that $P_{t,k}$ converges toward $1/2$.

It is possible to compute the exact value of $\#S_{t,k}$ for a given d and a corresponding set of β_is. It is worth noting that the order of the β_is does not matter because each subblock behaves the same when a is in $S_{t,k}$, i.e. it overflows. We did the computation for $d = 2$ where the symmetry of the problem leads to only one situation and gives a quite general result.

Definition 3.8.16.

$$f(x,y) = \frac{11}{27} + 4^{-x}\left(\frac{2}{9}x - \frac{2}{27}\right) + 4^{-y}\left(\frac{2}{9}y - \frac{2}{27}\right) + 4^{-x-y}\left(\frac{20}{27} - \frac{2}{9}(x+y)\right).$$

Proposition 3.8.17. *([104])*

$$P_{t,k} = f(\beta_1, \beta_2) \leq 1/2 \ .$$

Proof. An easy but quite lengthy and error-prone calculation, which can be checked with a symbolic calculus software, leads to the desired expression. The graph of f, computed with Maple^{TM} [208], is given in Fig. 3.3. □

We have proved:

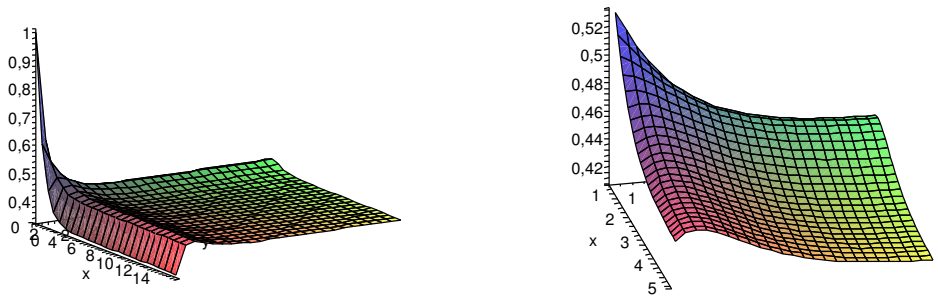

Figure 3.3 – Graph of $f(x, y)$.

Theorem 3.8.18. *([104]) If t verifies the following constraints:*

$$d = 2 \text{ and } \alpha_1, \alpha_2 \geq k - w_2(t) - 1 \ ,$$

then $\#S_{t,k} \leq 2^{k-1}$.

Finally, we have proved that a family of numbers reaches the bound (we believe they are the only ones to do so): In fact, we have added another constraint: $\forall i, \beta_i = 1$. The previous one becomes: $\min_i(\alpha_i) \geq k - w_2(t) - 1 = d - 1$.

Theorem 3.8.19. *[104] Let t verify the two following constraints:*

$$\forall i, \beta_i = 1 \text{ and } \min_i(\alpha_i) \geq k - w_2(t) - 1 = d - 1 \ ,$$

then $\#S_{t,k} = 2^{k-1}$.

Next we proved the conjecture in the following case:

Corollary 3.8.20. *Let t verify the two following constraints:*

$$\forall i, \alpha_i = 1 \text{ and } \min_i(\beta_i) \geq w_2(t) - 1 = d - 1 \ ,$$

then $\#S_{t,k} \leq 2^{k-1}$.

The theoretical study of the conjecture, together with experimental results obtained with Sage [241] made by Jean-Pierre Flori, lead to conjecture that the converse of Theorem 3.8.19 is also true, i.e. the numbers of Theorem 3.8.19 are the only ones reaching the bound of the Conjecture Tu-Deng, which is obviously stronger than the original conjecture.

Conjecture 3.8.21. *Let $k \geq 2$ and $t \in \left(\mathbb{Z}/(2^k - 1)\mathbb{Z}\right)^*$. Then $S_{t,k} = 2^{k-1}$ if and only if t verifies the two following constraints:*

- $\forall i, \ \beta_i = 1$,
- $\min_i(\alpha_i) \geq B - 1 = d - 1$.

As far we know, the conjectures presented in this section are still open. Only the variation proposed by Tang, Carlet and Tang has been proved recently by Cohen and Flori [67].

Chapter 4

Bent functions

Contents

In Chapter 3 we emphasized the fact that a cryptographic Boolean function should verify several (contradictory) criteria. Constructing satisfying functions is therefore a difficult task, and trade-offs between the different criteria have to be made. In the present chapter, our approach will be slightly different: we solely focus on one criterion — nonlinearity — and more precisely on functions achieving maximum nonlinearity: *bent* functions. Recall that the significance of this

aspect has again been demonstrated by the recent development of linear cryptanalysis initiated by Matsui [184, 183]. It is therefore especially important when Boolean functions are used as part of S-boxes in symmetric cryptosystems.

In the mathematical field of combinatorics, a bent function is a special type of Boolean function. Defined and named in the 1960's by Oscar Rothaus [227] in research not published until 1976, bent functions are so called because they are as different as possible from all linear and affine functions. The definition can be extended in several ways, leading to different classes of generalized bent functions that share many of the useful properties of the original.

4.1 Definition and properties

Recall that the *nonlinearity* of a Boolean function f, denoted by $nl(f)$, is the minimum Hamming distance between f and all affine functions. In figure 4.1, we give the distribution of all 4-variable Boolean functions with respect to its nonlinearity.

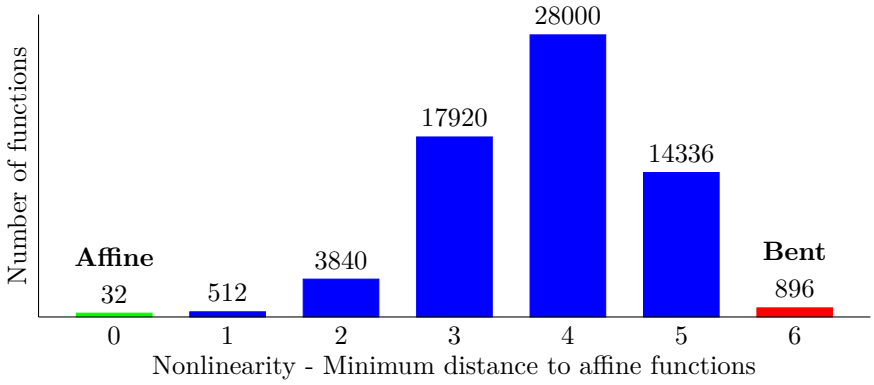

Figure 4.1 – Distribution of all 4-variable to nonlinearity

A powerful mathematical tool to measure the nonlinearity of a Boolean function is the *Walsh transform*. The nonlinearity of an n-variable Boolean function can be expressed by means of the Walsh transform as follows:

$$nl(f) = 2^{n-1} - \frac{1}{2} max_{b \in \mathbb{F}_2^n} |\widehat{\chi_f}(b)|.$$

Because of the well-known Parseval's relation $\sum_{b \in \mathbb{F}_2^n} \widehat{\chi_f}(b)^2 = 2^{2n}$, $nl(f)$ is upper bounded by $2^{n-1} - 2^{n/2-1}$. This bound is tight for n even.

Definition 4.1.1. *Let n be an even integer. An n-variable Boolean function is called bent if the upper bound $2^{n-1} - 2^{n/2-1}$ on its nonlinearity $nl(f)$ is achieved with equality.*

Consequently, we have the following main characterization (which is independent of the choice of the inner product on $\mathbb{F}_2^n$) of the bentness for Boolean functions:

Proposition 4.1.2. *Let n be an even integer. An n-variable Boolean function f is then bent if and only if its Walsh transform satisfies $\widehat{\chi_f}(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$.*

Hence, the Walsh–Hadamard transform provides a basic characterization of bentness. However, it can definitely not be used in practice to test efficiently bentness of a given function, especially

if all its values are computed naively one at a time as exponential sums. Nevertheless, it should be noted that all the values of the Walsh–Hadamard transform can be computed *at once* using the so-called fast Walsh–Hadamard transform, a kind of Fast Fourier Transform. The complexity of the fast Walsh–Hadamard transform is $O(2^n n^2)$ bit operations and $O(2^n n)$ memory [2] which limits the calculations at the most to $n = 40$.

In the following, we present the main properties of bent functions:

• The algebraic degree of any bent Boolean function on $\mathbb{F}_{2^n}$ is at most m (in the case that $n = 2$, the bent functions have degree 2).

•The set of n-variable bent Boolean functions is invariant under the action of the general affine group of $\mathbb{F}_{2^n}$ and the addition of n-variable affine Boolean functions. In particular, if f and f' are two n-variable Boolean functions such that f' is linearly equivalent to f (that is, there exists an $\mathbb{F}_2$-linear automorphism L of $\mathbb{F}_{2^n}$ such that $f' = f \circ L$) then, f is bent if and only if f' is bent.

• The automorphism group of the set of bent functions (i.e., the group of permutations π on $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ such that $f \circ \pi$ is bent for every bent function f) is the general affine group, that is, the group of linear automorphisms composed by translations [31]. The corresponding notion of equivalence between functions is called *affine equivalence*. Also, if f is bent and ℓ is affine, then $f + \ell$ is bent. A class of bent functions is called a *complete class* if it is globally invariant under the action of the general affine group and under the addition of affine functions. The corresponding notion of equivalence is called *extended affine equivalence*, in brief, *EA-equivalence*.

• Any function f is bent if and only if, for any nonzero vector a, the Boolean function, called the *derivative* at a $D_a f(x) = f(x) + f(x+a)$ is balanced (i.e. has Hamming weight 2^{n-1}). For this reason, bent functions are also called *perfect nonlinear functions*. Equivalently, f is bent if and only if the $2^n \times 2^n$ matrix $H = [(-1)^{f(x+y)}]_{x,y \in \mathbb{F}_2^n}$ is a Hadamard matrix (*i*.e. satisfies $H \times H^t = 2^n I$, where I is the identity matrix), and if and only if the support of f is a *difference set*. Bent functions have also the property that, for every even positive integer w, the sum $\sum_{a \in \mathbb{F}_2^n} \widehat{\chi_f}^{\,w}(a)$ is minimum.

• Bent Boolean functions always occur in pairs. In fact, given a bent function f on $\mathbb{F}_{2^n}$, we define the *dual Boolean function* $\widetilde{f}$ of f by considering the signs of the values $\widehat{\chi_f}(a), a \in \mathbb{F}_{2^n}$ of the Walsh transform of f as follows: $\widehat{\chi_f}(x) = 2^{\frac{n}{2}}(-1)^{\widetilde{f}(x)}$. Due to the involution law the Fourier transform is self-inverse. Thus, the dual $\widetilde{f}$ of a bent function f is again a bent function and its own dual is f itself.

4.2 Bent functions: applications

Bent functions have been extensively studied for their applications in cryptography, but have also been applied to spread spectrum[1] (it was discovered in early 1982 that maximum length sequences based on bent functions have cross-correlation and autocorrelation properties rivalling those of the Gold codes and Kasami codes for use in CDMA; these sequences have several applications

[1]In telecommunications and radio communication, spread-spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated in a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density (e.g. in satellite downlinks).

in spread spectrum techniques), coding theory, and combinatorial design[2]. The definition can be extended in several ways, leading to different classes of generalized bent functions that share many of the useful properties of the original. In the following, we precise only their uses in coding theory and symmetric cryptography.

4.2.1 Bent functions in coding theory

For every $0 \leq r \leq n$, the *Reed-Muller code* $\mathcal{RM}(r,n)$ of order r, is a linear code of length 2^n, dimension $\sum_{i=0}^{r} \binom{n}{i}$ and minimum distance 2^{n-r}. The Reed-Muller code can be defined in terms of Boolean functions or as extended cyclic code. In terms of Boolean functions, $\mathcal{RM}(r,n)$ is the set of all n-variable Boolean functions of algebraic degrees at most r. More precisely, it is the linear code of all binary words of length 2^n corresponding to the last columns of the truth-tables of these functions. The Reed-Muller codes are nested : $\mathcal{RM}(1,n) \subset \mathcal{RM}(2,n) \subset \cdots \subset \mathcal{RM}(n-1,n)$. The Reed-Muller code $\mathcal{RM}(r,n)$ can be viewed as an extended cyclic codes for every $r < n$: the zeroes of the corresponding cyclic code ($RM^{\star}(r,n)$, the *punctured Reed-Muller code* of order r) are the elements α^j (where α is a primitive element of $\mathbb{F}_{2^n}$) such that $1 \leq j \leq 2^n - 2$ and $1 \leq w_2(j) \leq n - r - 1$, where $w_2(j)$ is the number of ones in the binary expansion of j. Recall that given two Boolean functions f and g of $\mathcal{B}_n$, the *Hamming distance* $d_H(f,g)$ between f and g equals the size of the set $\{x \in \mathbb{F}_2^n \,|\, f(x) \neq g(x)\}$. Moreover, recall that $nl_r(f)$ denote the minimum Hamming distance between a given Boolean function f and all Boolean functions g of degrees at most r (that is, $g \in \mathcal{RM}(r,n)$). The covering radius of $\mathcal{RM}(r,n)$ denoted by $\rho(r,n)$ plays an important role in error correcting codes (see *e.g.* [68]). It is defined as the maximum value of $nl_r(f)$ when f ranges over the set $\mathcal{B}_n$ of Boolean functions in n variables, that is,

$$\rho(r,n) \;=\; \max_{f \in \mathcal{B}_n} \min_{g \in \mathcal{RM}(r,n)} d_H(f,g)$$

The covering radius $\rho(1,n)$ of the first-order Reed-Muller codes $\mathcal{RM}(1,n)$ coincides with the maximum nonlinearity $nl_1(f)$ (that we denoted simply by $nl(f)$) of n-variable Boolean functions f, that is, the maximum distance from all affine functions. When n is even, it is known that $\rho(1,n) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and the associated n-variable Boolean functions are the *bent functions*.

4.2.2 Bent functions in cryptography

The properties of bent functions are naturally of interest in modern digital cryptography. By 1988 Forré recognized that the Walsh transform of a function can be used to show that it satisfies the Strict Avalanche Criterion (SAC) and higher-order generalizations, and recommended this tool to select candidates for good S-boxes achieving near-perfect diffusion. Indeed, the functions satisfying the SAC to the highest possible order are always bent. Moreover, the bent functions are as far as possible from having what are called linear structures, nonzero vectors a such that $f(x+a)+f(x)$ is a constant. In the language of differential cryptanalysis (introduced after this property was discovered) the derivative of a bent function f at every nonzero point a (that is, $D_a(x) = f(x+a)+f(x)$) is a balanced Boolean function, taking on each value exactly half of the time. This property is called perfect nonlinearity. Given such good diffusion properties, apparently perfect resistance to differential cryptanalysis, and resistance by definition to linear cryptanalysis, bent functions might at first seem the ideal choice for secure cryptographic functions such as S-boxes. Their fatal flaw is that they fail to be balanced. In particular, an invertible S-box cannot be constructed directly from bent functions. Instead, one might start with a bent function and

[2]Combinatorial design theory is the part of combinatorial mathematics that deals with the existence and construction of systems of finite sets whose intersections have specified numerical properties.

n	2	4	6	8
# of bent functions	$8 = 2^3$	$896 = 2^{9.8}$	$5,425,430,528$	
$\approx$			$2^{32.3}$	$2^{106.3}$

Table 4.1 – Number of n-variable Bent functions for $2 \leq n \leq 8$

randomly complement appropriate values until the result is balanced. The modified function still has high nonlinearity, and as such functions are very rare the process should be much faster than a brute-force search. But functions produced in this way may lose other desirable properties, even failing to satisfy the SAC -so careful testing is necessary. A number of cryptographers have worked on techniques for generating balanced functions that preserve as many of the good cryptographic qualities of bent functions as possible. Some of this theoretical research has been incorporated into real cryptographic algorithms. The CAST design procedure, used by Carlisle Adams and Stafford Tavares to construct the S-boxes for the block ciphers CAST-128 and CAST-256, makes use of bent functions. The cryptographic hash function HAVAL uses Boolean functions built from representatives of all four of the equivalence classes of bent functions on six variables. The stream cipher Grain uses an NLFSR whose nonlinear feedback polynomial is, by design, the sum of a bent function and a linear function. Finally, it is important to note that a stream cipher using a bent function is vulnerable to correlation attacks in the combiner model and is also vulnerable to fast algebraic attacks and to Rønjom-Helleseth's attack [226] for the two models (the filter model and the combiner model).

4.3 Classification and enumeration of bent functions

The bent functions are a small set of Boolean functions and they are very valuable in particular for cryptography. Bent functions are all known for $n \leq 8$, only (their determination for 8 variables has been achieved only recently by Langevin and Leander [215] [3] as well as their classification under the action of the general affine group. We give in Table 4.1 the number of n-variable bent functions for $2 \leq n \leq 8$.

For $n \geq 10$, only classes of bent functions are known, which do not cover a large part of them, apparently. Determining all bent functions (or more practically, classifying them under the action of the general affine group) seems elusive. As we will see below, some infinite classes of bent functions have been obtained, thanks to the identification between the vectorspace $\mathbb{F}_2^n$ and the Galois field $\mathbb{F}_{2^n}$. Currently, the general structure of bent functions on $\mathbb{F}_{2^n}$ is not yet clear. In particular a complete classification of bent functions looks hopeless. Bent functions which are characterized as very rare, they are a vanishingly small fraction of the total number of functions when the number of variables increases. It stated in the litterature that there is no formal method of constructing all bent functions.

4.4 Construction of bent functions

4.4.1 Two main general constructions of bent functions

Several classes of bent functions have been introduced in [82, 227]. Some (like the $\mathcal{PS}$ class, recalled below) need conditions whose realizations are difficult to achieve, and so are more principles of constructions rather than explicit constructions. Others lead to explicit bent functions (given by

[3] the number of 8-variable bent functions equals 99270589265934370305785861242880

their ANF or their polynomial representation, univariate or bivariate). The two main ones of this last kind are the Maiorana-McFarland's constructions and the Partial Spread class $\mathcal{PS}_{ap}$.

- The Maiorana-McFarland's constructions are the best known primary constructions of bent functions is ([185, 82]). The *Maiorana-McFarland class* (denoted by $\mathcal{M}$) is the set of all the n-variable Boolean functions of the form:

$$f(x,y) = x \cdot \pi(y) + g(y);\ x, y \in \mathbb{F}_2^m \tag{4.1}$$

where "$\cdot$" denotes an inner product in $\mathbb{F}_2^m$, π is any permutation on $\mathbb{F}_2^m$ and g is any Boolean function on $\mathbb{F}_2^m$. Any such function is bent (the bijectivity of π is a necessary and sufficient condition for f being bent). The dual function $\widetilde{f}(x,y)$ equals: $y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$, where π^{-1} is the inverse of π. The completed class of $\mathcal{M}$ (that is, the smallest possible complete class including $\mathcal{M}$) contains all the quadratic bent functions (that is, the bent functions of algebraic degree 2) which are simple and best understood.

Proposition 4.4.1. *[82] A bent function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ belongs to the completed class of $\mathcal{M}$ if and only if there exists an $n/2$-dimensional vector subspace V in $\mathbb{F}_{2^n}$ such that the second-order derivatives*

$$D_{a,b}f(t) = f(t+a+b) + f(t+a) + f(t+b) + f(t)$$

vanish for any $a, b \in V$.

- The *Partial Spread class* $\mathcal{PS}$ introduced in [82] by Dillon is the set of all the sums (modulo 2) of the indicators of 2^{m-1} or $2^{m-1}+1$ pairwise supplementary m-dimensional subspaces of $\mathbb{F}_{2^n}$. All these functions are bent. Dillon denotes by $\mathcal{PS}^-$ (resp. $\mathcal{PS}^+$) the class of those $\mathcal{PS}$ functions for which the number of m-dimensional subspaces is 2^{m-1} (resp. $2^{m-1}+1$). We recall in the following result du to Dillon ([82], pp 95-100) (see also, for instance, Theorem 1 in [54]).

Theorem 4.4.2. *Let E_i, $i = 1, 2, \cdots, N$, be N subspaces of $\mathbb{F}_{2^n}$ of dimension m satisfying $E_i \cap E_j = \{0\}$ for all $i, j \in \{1, 2, \cdots, N\}$ with $i \neq j$. Let f be a Boolean function over $\mathbb{F}_{2^n}$ ($n = 2m$). Assume that the support of f can be written as*

$$supp(f) = \bigcup_{i=1}^{N} E_i^\star, \qquad \text{where } E_i^\star := E_i \setminus \{0\}$$

Then, f is bent if and only if $N = 2^{m-1}$. In this case f is said to be in the $\mathcal{PS}^-$ class.

All the elements of $\mathcal{PS}^-$ have algebraic degree m exactly, but not all those of $\mathcal{PS}^+$ (for instance, if m is even, then all quadratic functions are in $\mathcal{PS}^+$).

J. Dillon exhibits in [82] a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$ whose elements are defined in an explicit form:

Definition 4.4.3. *Let $n = 2m$ and let $\mathbb{F}_{2^n}$ be identified, as a vector space, with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ (thanks to the choice of a basis of the two-dimensional vector space $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$). The Partial Spread class $\mathcal{PS}_{ap}$ consists of all the functions f defined as follows: let g be a balanced Boolean function over $\mathbb{F}_{2^m}$ (ie. $wt(g) = 2^{m-1}$) such that $g(0) = 0$ (but, in fact, this last condition is not necessary for f to be bent). Then f is defined from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_2$ as $f(x,y) = g(\frac{x}{y})$ (i.e $g(xy^{2^m-2})$) with $\frac{x}{y} = 0$ if $y = 0$.*

The complements $g\left(\frac{x}{y}\right)+1$ of these functions are the functions $g(\frac{x}{y})$ where g is balanced and does not vanish at 0; they belong to the class $\mathcal{PS}^+$. In both cases, the dual of $g(\frac{x}{y})$ is $g(\frac{y}{x})$. The functions from class $\mathcal{PS}_{ap}$ are the functions whose supports are the unions of 2^{m-1} multiplicative cosets of $\mathbb{F}_{2^m}^\star$. These supports can be uniquely written as $\bigcup_{u\in S} u\mathbb{F}_{2^m}^\star$ where U is the set $\{u\in\mathbb{F}_{2^n}; u^{2^m+1}=1\}$ and S is a subset of U of size 2^{m-1}. We shall also include in $\mathcal{PS}_{ap}$ the complements of these functions.

4.4.2 Primary constructions and characterization of bent functions in polynomial forms

A number of researchers have been interested in providing construcions of bent functions in polynomial form that is, functions f whose expression is of the form (see Subsection 1.2.3, Chapter 1):

$$f(x)=\sum_{j\in\Gamma_n}\mathrm{Tr}_1^{o(j)}\left(a_jx^j\right)+\epsilon(1+x^{2^n-1}),\quad a_j\in\mathbb{F}_{2^{o(j)}}$$

Since the algebraic degree of any bent function over $\mathbb{F}_{2^n}$ is at most $\frac{n}{2}$, the Hamming weight of f is then even, that is, ϵ equals 0. Consequently, the polynomial form of any bent function f is of type:

$$f(x)=\sum_{j\in\Gamma_n}\mathrm{Tr}_1^{o(j)}\left(a_jx^j\right),\quad a_j\in\mathbb{F}_{2^{o(j)}}$$

The *monomial functions* and *binomial functions* are particular cases of functions in polynomial form. Monomial functions are functions which are the traces of a single power function, that is, functions f defined on $\mathbb{F}_{2^n}$ whose expression is of the form $f(x)=\mathrm{Tr}_1^n(ax^s)$ for given positive integer s and for some $a\in\mathbb{F}_{2^n}$. Binomial functions are functions f defined on $\mathbb{F}_{2^n}$ whose expression is of the form $f(x)=\mathrm{Tr}_1^n\left(a_1x^{s_1}+a_2x^{s_2}\right)$, $(a_1,a_2)\in(\mathbb{F}_{2^n}^\star)^2$ for a given positive integers s_1 and s_2 and for some coefficients a_1, a_2 in $\mathbb{F}_{2^n}$.

Monomial bent functions

As a first step towards a characterization of the trace forms of of bent functions, many authors focus on monomial functions, that is, functions whose the expression is of the form $\mathrm{Tr}_1^n(ax^s)$ for a given positive integer s and for some $a\in\mathbb{F}_{2^n}$. A *bent exponent* (always understood modulo 2^n-1) is an integer s such that there exists $a\in\mathbb{F}_{2^n}^\star$ for which $x\mapsto\mathrm{Tr}_1^n(ax^s)$ is bent. The current list of known bent exponents is given in table I. We send the readers to [159] where known cases of monomial bent functions are presented. Canteaut *et. al* [21] have carried out an exhaustive search and shown that there is no other exponent s for $n\leq 20$. The complete classification of monomial bent functions is not yet achieved.

exponent	condition	Family	References
2^i+1	$\frac{n}{gcd(n,i)}$ even	$\mathcal{M}$	[112]
$a(2^{\frac{n}{2}}-1)$	$gcd(a,2^{\frac{n}{2}}+1)=1$	PS_{ap}	[82, 156, 159, 54]
$2^{2i}-2^i+1$	$gcd(i,n)=1$		[84]
$(2^{\frac{n}{4}}+1)^2$	$n=4r$, r odd	$\mathcal{M}$	[58, 159]
$2^{\frac{n}{3}}+2^{\frac{n}{6}}+1$	$n\equiv 0 \mod 6$	$\mathcal{M}$	[21]

Table 4.2 – Bent Exponent

Note that the cyclotomic cosets modulo 2^n-1 of all the bent exponents presented in table 4.2 are of maximal size n that is, $o(s)=n$. The corresponding monomial functions are then in polynomial forms.
A monomial function $f(x)=\mathrm{Tr}_1^n(ax^s)$ cannot be bent for every non-zero a (see *e.g.* [159]). Moreover, there are some necessary conditions for s to be a bent exponent (see for instance [159]):

- the 2-weight of a bent exponent s is at most $\frac{n}{2}$.
- $gcd(s,2^n-1)>1$; moreover, $gcd(s,2^{\frac{n}{2}}-1)=1$ or $gcd(s,2^{\frac{n}{2}}+1)=1$.

Remark 4.4.4. *Note that bent functions have been also obtained by Dillon and McGuire [85] as the restrictions of functions on $\mathbb{F}_{2^{n+1}}$, with $n+1$ odd, to a hyperplane of this field: these functions are the Kasami functions $\mathrm{Tr}_1^n(x^{2^{2k}-2^k+1})$ and the hyperplane has equation $\mathrm{Tr}_1^n(x)=0$. The restriction is bent under the condition that $n+1=3k\pm 1$.*

We have looked for the exponents s such that $o(s)<n$ for which there exists at least one coefficient $a\in\mathbb{F}_{2^{o(s)}}$ such that, the Boolean function $\mathrm{Tr}_1^{o(s)}(ax^s)$ is bent. After an exhaustive search up to $n\leq 14$, we have found that, the only bent Boolean functions belonging the set of monomial functions with exponent s such that $o(s)<n$ are of the form $\mathrm{Tr}_1^{\frac{n}{2}}(ax^{2^{\frac{n}{2}}+1})$, for some $a\in\mathbb{F}_{2^n}$. Such functions have been given by Yu and Gong in [273]. Note that a class of quadratic functions (*i.e.* of algebraic degree 2) defined on $\mathbb{F}_{2^n}$ whose expression has the form: $f(x)=\sum_{i=1}^{\frac{n}{2}-1}a_i\,\mathrm{Tr}_1^n(x^{1+2^i})+a_{\frac{n}{2}}\,\mathrm{Tr}_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}}+1})$ with $a_i\in\mathbb{F}_2$, for $i\in\{1,\ldots,\frac{n}{2}\}$, was considered in several papers, in which the authors investigate the conditions on the choice of the coefficients a_i for explicit definition of an infinite class of quadratic bent functions. A non-exhaustive list of references which deals with the characterization of the bentness of this class is [144, 151, 173, 59, 273, 134].

Binomial bent functions with Niho exponents

Some constructions of binomial bent functions via Niho power functions have been given in [93]. Recall that a positive integer s (always understood modulo 2^n-1) is said to be a *Niho exponent*, and x^s a *Niho power function*, if the restriction of x^s to $\mathbb{F}_{2^m}$ is linear or in other words $s\equiv 2^j \pmod{2^m-1}$ for some $j<n$. As we consider $\mathrm{Tr}_1^n(x^d)$, without loss of generality, we can assume that s is in the normalized form, with $j=0$, and then we have a unique representation $s=(2^m-1)d+1$ with $2\leq d\leq 2^m$. The name of Niho exponent comes from a theorem dealing with power functions by Niho [220], which has been later extended to linear combinations of such power functions in [93] (see also [160]), and which relates the value of the Walsh transform of such sum to the number of solutions in U of some equation. According to Dobbertin *et. al.* [93], three subfamilies containing bent functions can be identified in the set of binomial functions (the fractions are interpreted modulo 2^m+1, for instance $\frac{1}{2}=2^{m-1}+1$):

- $s_1=(2^m-1)\frac{1}{2}+1$ and $s_2=(2^m-1)3+1$;
- $s_1=(2^m-1)\frac{1}{2}+1$ and $s_2=(2^m-1)\frac{1}{4}+1$ (m odd);
- $s_1=(2^m-1)\frac{1}{2}+1$ and $s_2=(2^m-1)\frac{1}{6}+1$ (m even).

The following statement summarizes the results given in [93].

Theorem 4.4.5. *([93]) Let $n=2m$. Let f be a function defined on $\mathbb{F}_{2^n}$ of the form $f(x)=\mathrm{Tr}_1^n\left(a_1x^{(2^m-1)\frac{1}{2}+1}+a_2x^{s_2}\right)$, where a_1, $a_2\in\mathbb{F}_{2^n}^\star$. Assume that $a_2^{\frac{2^m+1}{2}}=a_1+{a_1}^{2^m}$.*

1. *Let $s_2=(2^m-1)3+1$. If $a_2=\gamma^5$ for some $\gamma\in\mathbb{F}_{2^n}^\star$ then, f is a bent function of degree m (note that if $m\not\equiv 2 \pmod 4$ then, the map $x\mapsto x^5$ is a permutation of $\mathbb{F}_{2^n}$).*

2. Suppose m is odd. Let $s_2 = (2^m - 1)\frac{1}{4} + 1$. Then f is a bent function of degree 3.

3. Suppose m is even. Let $s_2 = (2^m - 1)\frac{1}{6} + 1$. Then f is a bent function of degree m.

Note that as observed in [41], there is a mistake made in [93] (Theorem 3) while computing the algebraic degree of the third Niho bent function. Indeed the degree calculated in [93] being equal $\frac{m}{2} + 1$ is not correct. The correct degree is m and this comes from the following lemma.

Lemma 4.4.6. *([41]) Take even $m > 2$ and interpret $\frac{1}{3}$ as an inverse of 3 modulo $2^m + 1$. Then the exponent $2s_2 = (2^m - 1)\frac{1}{3} + 2$ has the binary weight m.*

Proof. First, note that 1/3 modulo $2^m + 1$ is equal to $(2^m + 2)/3$. Then

$$\begin{aligned} 2s_2 &= \frac{2^n - 1}{3} + \frac{2^m - 1}{3} + 2 \\ &= \sum_{i=0}^{m-1} 2^{2i} + \sum_{i=0}^{m/2-1} 2^{2i} + 2 \\ &= \sum_{i=0}^{m/2-1} 2^{2i+1} + \sum_{i=m/2}^{m-1} 2^{2i} + 2 \end{aligned}$$

whose binary weight equals m if $m > 2$. □

Remark 4.4.7. *Note that $o(s_1) = o((2^m - 1)\frac{1}{2} + 1) = \frac{n}{2}$ and $o(s_2) = n$ for $s_2 \in \{(2^m - 1)3 + 1, (2^m - 1)\frac{1}{4} + 1, (2^m - 1)\frac{1}{6} + 1\}$. The polynomial forms of the three binomial functions given in Theorem 4.4.5 are then in form*

$$\mathrm{Tr}_1^m(a_1{}' x^{2^m+1}) + \mathrm{Tr}_1^n(a_2 x^{s_2}), a_1{}' \in \mathbb{F}_{2^m}^\star \text{ and } a_2 \in \mathbb{F}_{2^n}^\star$$

The problem of knowing whether the duals of the binomial functions given in [93] are affine equivalent to these Niho bent functions was left open in [93]. Very recently, the bivariate representation (obtained by identifying $\mathbb{F}_{2^n}$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and we consider then the input to the Boolean function as an ordered pair $(x; y)$ of elements of $\mathbb{F}_{2^m}$) of the second Dobbertin-et-al's function and the bivariate expression of its dual have been computed in [44]. We also observed in [44] that the dual is not a Niho bent function, which allows replying negatively to the open question in [93]. We will discuss on the dual of those Niho bent functions in Subsection 4.8.1.

Binomial bent functions with Dillon (like) exponents

Chapter 5 is dealing with a more strong property than the bentness, more precisely, the hyper-bentness (since hyper-bent functions are in particular bent). The known constructions of bent functions via Dillon (like) exponents are also hyper-bent. So for the constructions of binomial bent functions we refer the reader to Subsection 5.5.2 in Chapter 5 in which we will present the known constructions of binomial hyper-bent functions.

Bent functions via several Niho exponents

The second class in [93] of binomial bent function (that is obtained with the exponent $(2^m - 1)\,3 + 1$) has been extended by Leander and Kholosha [160] into the functions:

$$\mathrm{Tr}_1^n\left(at^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} t^{s_i}\right)$$

where $r > 1$ such that $gcd(r, m) = 1$, $a \in \mathbb{F}_{2^n}$ such that $a + a^{2^m} = 1$, $s_i = (2^m - 1)\frac{i}{2^r} + 1 \pmod{2^m + 1}$, $i \in \{1, \ldots, 2^{r-1} - 1\}$.

Bent functions with multiple trace terms via Dillon (like) exponents

The known bent functions whose expressions are multiple trace terms via Dillon (like) exponents are also hyper-bent. So, we refer the reader to Chapter 6.

4.4.3 Secondary constructions of bent functions

In this subsection, we refer to Carlet's chapter [31] (Subsection 6.4.2). There exist several secondary constructions of bent functions but the best-known constructions are those of Rothaus ("direct sum") and of Carlet ("indirect sum"). Since the author did not contribute in the secondary constructions of bent functions, we will not detail all the constructions but we will just mention them briefly. We advise the reader who is interessed in this direction to referred to Carlet's chapter [31].
1. The first secondary construction was given by Dillon and Rothaus ([82, 227]). Such a construction is called the *direct sum* and is defined as follows: let f be a bent function on $\mathbb{F}_2^n$ (n even) and g a bent function on $\mathbb{F}_2^m$ (m even) then the function h defined on $\mathbb{F}_2^{n+m}$ by $h(x, y) = f(x) \oplus g(y)$ is bent. Unfortunately this construction has no great interest from a cryptographic point of view[4]
2. Dillon and Rothaus have proved the more interesting construction defined as follows: following: if g, h, k and $g \oplus h \oplus k$ are bent on $\mathbb{F}_2^n$ (n even), then the function defined at every element (x_1, x_2, x) of $\mathbb{F}_2^{n+2}$ ($x_1, x_2 \in \mathbb{F}_2$, $x \in \mathbb{F}_2^n$) by:

$$f(x_1, x_2, x) =$$

$$g(x)h(x) \oplus g(x)k(x) \oplus h(x)k(x) \oplus [g(x) \oplus h(x)]x_1 \oplus [g(x) \oplus k(x)]x_2 \oplus x_1x_2$$

is bent. Unfortunately no general class of bent functions has been deduced from this construction.

3. Carlet has proposed in [24] the two classes of bent functions which are derived from Maiorana-McFarland's class, by adding to some functions of this class the indicators of some vector subspaces. The result of Carlet is the following.

Theorem 4.4.8. *([24]) Let $b + E$ be any flat in $\mathbb{F}_2^n$ (E being a linear subspace of $\mathbb{F}_2^n$). Let f be any bent function on $\mathbb{F}_2^n$. The function $f^\star = f \oplus 1_{b+E}$ is bent if and only if one of the following equivalent conditions is satisfied:*

1. *For any a in $\mathbb{F}_2^n \setminus E$, the function $D_a f$ is balanced on $b + E$;*
2. *The restriction of the function $\widetilde{f}(x) \oplus b \cdot x$ to any coset of $E^\perp$ is either constant or balanced.*

If f and $f^\star$ are bent, then E has dimension greater than or equal to $n/2$ and the algebraic degree of the restriction of f to $b + E$ is at most $\dim(E) - n/2 + 1$.
If f is bent, if E has dimension $n/2$, and if the restriction of f to $b + E$ has algebraic degree at most $\dim(E) - n/2 + 1 = 1$, i.e. is affine, then conversely $f^\star$ is bent too.

4. Other classes of bent functions have been deduced from a construction given by Carlet in [26], which generalizes the secondary constructions given in 1 and 2 above:

[4] in fact, this construction produces decomposable functions (a Boolean function is called decomposable if it is equivalent to the sum of two functions that depend on two disjoint subsets of coordinates; such peculiarity is easy to detect and can be used for designing divide-and-conquer attacks, as pointed out by J. Dillon in [82])

Theorem 4.4.9. *([26]) Let n and m be two even positive integers. Let f be a Boolean function on $\mathbb{F}_2^{n+m} = \mathbb{F}_2^n \times \mathbb{F}_2^m$ such that, for any element y of $\mathbb{F}_2^m$, the function on $\mathbb{F}_2^n$:*

$$f_y : x \mapsto f(x, y)$$

is bent. Then f is bent if and only if, for any element s of $\mathbb{F}_2^n$, the function

$$\varphi_s : y \mapsto \widetilde{f_y}(s)$$

is bent on $\mathbb{F}_2^m$. If this condition is satisfied, then the dual of f is the function $\widetilde{f}(s,t) = \widetilde{\varphi_s}(t)$ (taking as inner product in $\mathbb{F}_2^n \times \mathbb{F}_2^m$: $(x,y)\cdot(s,t) = x\cdot s \oplus y \cdot t$).

The previous result give rise to a nice secondary construction due to Carlet ([28]) called the *indrect sum*:

Corollary 4.4.10. *[28]) Let f_1 and f_2 be two n-variable bent functions (n even) and let g_1 and g_2 be two m-variable bent functions (m even). Define*[5]

$$h(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)\,(g_1 \oplus g_2)(y);\ x \in \mathbb{F}_2^n,\ y \in \mathbb{F}_2^m.$$

Then h is bent and its dual is obtained from $\widetilde{f_1}, \widetilde{f_2}, \widetilde{g_1}$ and $\widetilde{g_2}$ by the same formula as h is obtained from f_1, f_2, g_1 and g_2.

5. A very simple observation of X.-D. Hou and P. Langevin have made in [132] leads to potentially new construction of bent functions (which does not increase the number of variables, contrary to most other secondary constructions).
6. Another secondary construction without extension of the number of variables have been introduced by Carlet in [29].

Theorem 4.4.11. *([29]) Let f_1, f_2 and f_3 be three n-variable bent functions, n even. Denote by s_1 the function $f_1 \oplus f_2 \oplus f_3$ and by s_2 the function $f_1f_2 \oplus f_1f_3 \oplus f_2f_3$. Then:*
- if s_1 is bent and if $\tilde{s_1} = \tilde{f_1} \oplus \tilde{f_2} \oplus \tilde{f_3}$, then s_2 is bent, and $\tilde{s_2} = \tilde{f_1}\tilde{f_2} \oplus \tilde{f_1}\tilde{f_3} \oplus \tilde{f_2}\tilde{f_3}$;
*- if $\widehat{s_{2_\chi}}(a)$ is divisible by $2^{n/2}$ for every a (*e.g. *if s_2 is bent, or if it is quadratic, or more generally if it is plateaued* [6]*, then s_1 is bent.*

7. Using the notion of normal extension of bent function, Carlet et al. [15] have proposed another secondary construction of bent functions.

4.5 Bent vectorial functions

Let n and r be two positive integers ($n \geq 1$, $r \geq 1$). An (n,r)-function F being given, the component functions of F are the Boolean functions $l \circ F$, where l ranges over the set of all the nonzero linear forms over $\mathbb{F}_2^r$. Equivalently, they are the linear combinations of a non-null number of their coordinate functions, that is, the functions of the form $v \cdot F, \quad v \in \mathbb{F}_2^r \setminus \{0\}$, where "$\cdot$" denotes the usual inner product in $\mathbb{F}_2^r$ (or any other inner product). The vector spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^r$ can be identified, if necessary, with the Galois fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^r}$ of orders 2^n and 2^r respectively. Hence, (n,r)-functions can be viewed as functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^r$ or as functions

[5] h is the concatenation of the four functions f_1, $f_1 \oplus 1$, f_2 and $f_2 \oplus 1$, in an order controled by $g_1(y)$ and $g_2(y)$. This construction $(f_1, f_2, g_1, g_2) \mapsto h$ leads to construct resilient functions (see [31]).

[6] the functions satisfying $nl(f) = 2^{n-1} - 2^{-n/2-1}\sqrt{\mathcal{V}(f)}$ (resp. $\mathcal{V}(f) \times N_{\widehat{f_\chi}} = 2^{3n}$) are the functions whose Walsh transforms take at most one nonzero magnitude. These functions are called plateaued functions.

from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$. In the latter case, the component functions are the functions $\mathrm{Tr}_1^r(vF(x))$. We recall some basic facts that we need about vectorial functions. Any (n,r)-function F admits a unique representation as a multivariate polynomial over $\mathbb{F}_2^r$, called its *algebraic normal form* (ANF), of the form:

$$F(x_1,\cdots,x_n)=\sum_{u\in\mathbb{F}_2^n} c(u)\left(\prod_{i=1}^{n} x_i^{u_i}\right), \quad c(u)\in\mathbb{F}_2^r.$$

The *algebraic degree* $\deg(F)$ of any (n,r)-function F is by definition the global degree of its ANF (ie. equals the maximum degree of those monomials whose coefficients are nonzero in its algebraic normal form). It also equals the maximum algebraic degree of the coordinate functions of F or of its component functions. Affine functions (resp. quadratic functions) are functions whose algebraic degree is a most 1 (resp. equals 2). Vectorial cryptographic functions must have high algebraic degree to withstand several kinds of attacks (mainly the higher order differential attack in the case of block ciphers and the Berlekamp-Massey attack in the case of stream ciphers).

If we identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, then, any (n,n)-function F is uniquely expressed as a univariate polynomial over $\mathbb{F}_{2^n}$, of degree at most 2^n-1:

$$F(x)=\sum_{j=0}^{2^n-1} c_j x^j \ , \quad c_j\in\mathbb{F}_{2^n} \ .$$

The algebraic degree of F is equal to $\max_{j/\,c_j\neq 0} w_2(j)$ where $w_2(j)$ is the *2-weight* of j, that is, the number of nonzero coefficients j_s in the binary expansion $\sum_{s=o}^{n-1} j_s 2^s$ of j.

For every integer r dividing n, an (n,r)-function F can be viewed as a function from $\mathbb{F}_{2^n}$ to itself and, therefore admits a unique univariate polynomial representation, which can be represented in the form $\mathrm{Tr}_r^n(\sum_{j=0}^{2^n-1} c_j x^j)$, where Tr_r^n is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$ (but without uniqueness if we do not add restrictions on the polynomial inside the brackets).

The notion of balancedness and bentness plays an important role for vectorial Boolean functions in cryptography.

Definition 4.5.1. *An (n,r)-function F is called balanced if it takes every value of $\mathbb{F}_2^r$ the same number 2^{n-r} of times. Equivalently, F is balanced if for every $b\in\mathbb{F}_2^r$, the Boolean function ϕ_b defined on $\mathbb{F}_2^n$ by $\phi_b(x)=1$ if $F(x)=b$ and $\phi_b(x)=0$ otherwise, has Hamming weight 2^{n-r}.*

The balanced vectorial functions can be characterized by the balancedness of their component (Boolean) functions as follows.

Proposition 4.5.2. *An (n,r)-function F is balanced if and only if its component functions are balanced, that is, if for every nonzero $v\in\mathbb{F}_2^r$, the Boolean function $v\cdot F$ on $\mathbb{F}_2^n$ is balanced (i.e has Hamming weight 2^{n-1}).*

The notion of Walsh transform is defined for vectorial functions as well. More precisely, given an (n,r)-function F, the Walsh transform of F is the function which maps any ordered pair $(a,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^r$ to the value at a of the Walsh transform of the component (Boolean) function $v\cdot F$ ($v\neq 0$), that is: $\widehat{\chi_{v\cdot F}}(a)=\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+x\cdot a}$, where the same symbol "$\cdot$" is used to denote inner products in $\mathbb{F}_2^r$ and in $\mathbb{F}_2^n$.

Generalized to (n,r)-functions, the nonlinearity is defined as the minimum nonlinearity of all their component functions $v\cdot F, v\in\mathbb{F}_2^r\setminus\{0\}$ and we have:

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{v\in\mathbb{F}_2^{r*};\ u\in\mathbb{F}_2^n} \left| \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot F(x)+u\cdot x} \right|.$$

The nonlinearity represents a measure for the resistance of S-Boxes against linear cryptanalysis [181]. In the case of stream ciphers, another notion of nonlinearity must also be considered: the minimum nonlinearity of all the Boolean functions of the form $\varphi \circ F$ where φ is any non-constant r-variable Boolean function (indeed a fast correlation attack can be performed on the cipher using any such $\varphi \circ F$ as Boolean filtering or combining function), but we shall not be interested in this notion in the present paper. The upper bound $2^{n-1} - 2^{n/2-1}$ on the nonlinearity of any n-variable Boolean function is obviously valid for (n, r)-functions.

Definition 4.5.3. *Let n be an even integer and r be an integer. An (n, r)-function F is called bent if the upper bound $2^{n-1} - 2^{n/2-1}$ on its nonlinearity $nl(F)$ is achieved with equality.*

Bent (n, r)-functions exist then only if n is even. But according to Nyberg [211], this condition is not sufficient for the existence of bent (n, r) functions. More precisely, bent (n, r)-functions exist if and only if n is even and $r \leq \frac{n}{2}$. Obviously, the bentness of vectorial functions can be characterized by the bentness of their component (Boolean) functions: an (n, r)-function F is bent if and only if all of the component functions of F are bent, that is, if $\widehat{\chi_{v\cdot F}}(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$ and for all $v \in \mathbb{F}_2^r \setminus \{0\}$. This is equivalent to the fact that, for every $v \in \mathbb{F}_2^r \setminus \{0\}$ and every $a \in \mathbb{F}_2^n \setminus \{0\}$, the function $v \cdot (F(x) + F(x + a))$ is balanced, which is itself (according to Characterization 1) equivalent to saying that the function $F(x) + F(x + a)$ is balanced. Hence, bent functions contribute to an optimal resistance to the differential attack as well. The notion of bent vectorial function is EA-invariant (recall that this means invariant under composition on the left and on the right by affine automorphisms and under addition of affine functions). It is well known that the algebraic degree of any bent (n, r)-function is at most $\frac{n}{2}$.

From now on, we assume the hypothesis "n is even and $r \leq \frac{n}{2}$" are satisfied on the ordered pair (n, r) when we consider bent (n, r)-functions.

4.5.1 Primary constructions of bent vectorial functions

Recall that constructions "from scratch" are called primary. On the contrary, secondary constructions will use already constructed functions to build new ones. There exist two general classes of bent Boolean functions, the Maiorana-McFarland class and the PS_{ap} class, which straightforwardly generalize to vectorial functions (this was first observed by Nyberg [211]).
1. Maiorana-McFarland's constructions of vectorial functions:

An n-variable Boolean bent function f belongs to the Maiorana-McFarland class if, up to EA-equivalence and writing its input in the form (x, y), with x, y in $\mathbb{F}_2^{n/2}$, the corresponding output equals $f(x, y) = x \cdot \pi(y) + g(y)$ (where "$\cdot$" is an inner product in $\mathbb{F}_2^{n/2}$), where π is a permutation of $\mathbb{F}_2^{n/2}$ and g is a Boolean function on $\mathbb{F}_2^{n/2}$. The bijectivity of π is a necessary and sufficient condition for the bentness of a Boolean function of the form $x \cdot \pi(y) + g(y)$. It it well known that all the quadratic bent Boolean functions belong to the Maiorana-McFarland class of Boolean (bent) functions. In the following, we shall see that three versions (of different levels of generality) can be given for the extension of this construction to vectorial functions.

• **The strict Maiorana-McFarland class:** We endow $\mathbb{F}_2^{n/2}$ with the structure of the field $\mathbb{F}_{2^{n/2}}$. We identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$. Any function of the form $F(x, y) = L(x\,\pi(y)) + G(y)$,

where the product $x\,\pi(y)$ is calculated in $\mathbb{F}_{2^{n/2}}$, where L is any linear or affine function from $\mathbb{F}_{2^{n/2}}$ onto $\mathbb{F}_2^r$, π is any permutation of $\mathbb{F}_{2^{n/2}}$ and G is any $(n/2,r)$-function, is an (n,r) bent function. We call *strict Maiorana-McFarland's class* the set of functions which are EA-equivalent to these functions.
An example is given in [244], whose i-th coordinate is defined as $f_i(x,y) = \mathrm{Tr}_1^{\frac{n}{2}}(x\,\pi_i(y)) + g_i(y)$, $x,y \in \mathbb{F}_{2^{n/2}}$, where g_i is any Boolean function on $\mathbb{F}_{2^{n/2}}$ and where

$$\pi_i(y) = \begin{cases} 0 \text{ if } y = 0 \\ \alpha^{dec(y)+i-1} \text{ otherwise} \end{cases},$$

with α a primitive element of $\mathbb{F}_{2^{n/2}}$ and $dec(y) = 2^{n/2-1}y_1 + 2^{n/2-2}y_2 + \cdots + y_{n/2}$. This function belongs to the strict Maiorana-McFarland class of bent functions because the function $y \mapsto \begin{cases} 0 \text{ if } y = 0 \\ \alpha^{dec(y)} \text{ otherwise} \end{cases}$ is a permutation from $\mathbb{F}_2^{n/2}$ to $\mathbb{F}_{2^{n/2}}$, and the function $L : x \in \mathbb{F}_{2^{n/2}} \mapsto (\mathrm{Tr}_1^{\frac{n}{2}}(x), \mathrm{Tr}_1^{\frac{n}{2}}(\alpha x), \cdots, \mathrm{Tr}_1^{\frac{n}{2}}(\alpha^{n/2-1}x)) \in \mathbb{F}_2^{n/2}$ is an isomorphism.

• **The extended Maiorana-McFarland class:** Let F be any function of the form

$$F : (x,y) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \mapsto \psi(x,y) + G(y) \in \mathbb{F}_2^m,$$

where G is any function from $\mathbb{F}_2^{n/2}$ to $\mathbb{F}_2^m$ and $\psi : \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \mapsto \mathbb{F}_2^m$ is such that, for every $y \in \mathbb{F}_2^{n/2}$, the function $x \mapsto \psi(x,y)$ is linear and, for every nonzero $x \in \mathbb{F}_2^{n/2}$, the function $y \mapsto \psi(x,y)$ is balanced. Then F is bent. Indeed, for every nonzero $v \in \mathbb{F}_2^m$ and every $y \in \mathbb{F}_2^{n/2}$, there exists a unique vector v_y such that $v \cdot \psi(x,y) = x \cdot v_y$. The nonzero vector v being fixed, the function $y \mapsto v_y$ is bijective if and only if, for every $x \neq 0$, the function $y \mapsto x \cdot v_y$ is balanced (indeed, a vectorial function is balanced if and only if all its component functions are balanced), that is, the function $y \mapsto v \cdot \psi(x,y)$ is balanced. This property is achieved for every nonzero $v \in \mathbb{F}_2^m$ if and only if, for every nonzero $x \in \mathbb{F}_2^{n/2}$, the function $y \mapsto \psi(x,y)$ is balanced. Then, for any $u,u' \in \mathbb{F}_2^{n/2}$, the value at (u,u') of the Walsh transform $\widehat{\chi_{v\cdot F}}$ of the component function $v \cdot F$ of F is equal to

$$\begin{aligned} \sum_{(x,y)\in\mathbb{F}_2^{n/2}\times\mathbb{F}_2^{n/2}} (-1)^{v\cdot\psi(x,y)+v\cdot G(y)+u\cdot x+u'\cdot y} &= 2^{n/2} \sum_{y\in\mathbb{F}_2^{n/2}/\, v_y=u} (-1)^{v\cdot G(y)+u'\cdot y} \\ &= \pm 2^{n/2}. \end{aligned}$$

We call *extended Maiorana-McFarland's class* the set of functions which are EA-equivalent to these functions. It includes the strict class.
An example of function ψ is $\psi(x,y) = \varphi(x,\pi(y))$, where π is a permutation of $\mathbb{F}_2^{n/2}$ and φ is any $\mathbb{F}_2$-bilinear (non-necessarily symmetric) function such that, for every nonzero $x \in \mathbb{F}_2^{n/2}$ and every nonzero $y \in \mathbb{F}_2^{n/2}$, we have $\varphi(x,y) \neq 0$. Indeed, this condition is necessary and sufficient for the linear function $y \mapsto \varphi(x,y)$ to be balanced over $\mathbb{F}_{2^{n/2}}$ for every nonzero x.
An example of such φ over the field $\mathbb{F}_{2^{n/2}}$ and with $m = n/2$ is obviously $\varphi(x,y) = x\,y$ but other examples exist. For instance, $\varphi(x,y) = x^4y + wxy^4$, where $w \in \mathbb{F}_{2^{n/2}}$ works, if w is not a cube in $\mathbb{F}_{2^{n/2}}$ (which obliges us to take n divisible by 4) since $x^4y + wxy^4 = 0$ with $x,y \neq 0$ implies $w = (x/y)^3$.
Characterizing all functions $\psi(x,y) = \sum_{i=0}^{n/2-1} \psi_i(y)\,x^{2^i}$ such that the function $y \mapsto \psi(x,y)$ is balanced for all nonzero $x \in \mathbb{F}_2^{n/2}$ is an open problem, as far as we know.

Remark 4.5.4. *The (n,r)-functions above are given as defined over $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ (it is also the case for other functions, in particular those in the PS_{ap} class, see Section 2). And, we know that for r a divisor of n, any (n,r)-function can be viewed as a function from $\mathbb{F}_{2^n}$ to itself and, therefore, can be uniquely expressed as a univariate polynomial over $\mathbb{F}_{2^n}$. So, as mentioned in [23], in the case when $r = n/2$ the univariate representation of such functions can be easily obtained:*
- let w be any element in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$, we can write $X = x + wy \in \mathbb{F}_{2^n} = \mathbb{F}_{2^{n/2}} + w\mathbb{F}_{2^{n/2}}$ and we have then $y = \frac{X+X^{2^{n/2}}}{w+w^{2^{n/2}}}$ and $x = \frac{w^{2^{n/2}}X+wX^{2^{n/2}}}{w+w^{2^{n/2}}}$;
- in particular if $n/2$ is odd, we can choose for w a primitive element of $\mathbb{F}_4$ and we have then: $x = w^2X + wX^{2^{n/2}}$ and $y = X + X^{2^{n/2}}$.
For instance, the univariate representation of the simplest Maiorana-McFarland function, that is the function $(x,y) \mapsto xy$, is $(w^2X + wX^{2^{n/2}})(X + X^{2^{n/2}})$, that is, up to addition of linear terms: $X^{1+2^{n/2}}$ if $n/2$ is odd and equals this functions multiplied by a nonzero term if $n/2$ is even.

• **The general Maiorana-McFarland class** is the set of (n,r)-functions such that, for every $v \in \mathbb{F}_2^{r*}$, the component function $v \cdot F$ belongs, up to affine equivalence, to the Maiorana-McFarland class of Boolean bent functions. It straightforwardly includes the extended class. The general class contains all bent quadratic functions, since we know that, up to affine equivalence and addition of a constant, every quadratic n-variable bent Boolean function equals $x_1x_2+\cdots+x_{n-1}x_n$ [98].

Modifications of the Maiorana-McFarland bent functions have been proposed in [213].

2. Partial Spread constructions of vectorial functions:

We endow $\mathbb{F}_2^{n/2}$ with the structure of the field $\mathbb{F}_{2^{n/2}}$. We identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$. Recall that Boolean functions of the class PS_{ap} introduced by Dillon [83, 82] are bent. They are defined in an explicit form $f(x,y) = g(\frac{x}{y})$ with $(x,y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ and $\frac{x}{y} = 0$ if $y = 0$, where g is a Balanced Boolean function on $\mathbb{F}_{2^{n/2}}$. The balancedness of g is in fact a necessary and sufficient condition for f being bent. Moreover, the dual function $\widetilde{f}$ of f is the Boolean function defined, for every $(a,b) \in (\mathbb{F}_{2^n})^2$, by $\widetilde{f}(a,b) = g(\frac{b}{a})$, which belongs also to the class of PS_{ap}.

• **The PS_{ap} class of vectorial functions:** any function F over $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ defined by $F(x,y) := G(xy^{2^n-2}) = G\left(\frac{x}{y}\right)$ (with $\frac{x}{y} = 0$ if $y = 0$), $x, y \in \mathbb{F}_{2^{n/2}}$, where G is a balanced $(n/2,r)$-function, is a bent (n,r)-function (since for every $v \neq 0$, the component function $v \cdot F$ belongs to the class PS_{ap} of Dillon's functions).

• **A Partial Spread construction:** Let us recall a construction of Boolean bent functions proposed by Carlet:

Theorem 4.5.5. *([26]) Let n and m be two even integers. Let f be a Boolean function on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ such that, for any element y of $\mathbb{F}_2^m$ the Boolean function $f_y : x \in \mathbb{F}_2^n \mapsto f(x,y)$ is bent. Then, f is bent on $\mathbb{F}_2^{n+m}$ if and only if, for any element s of $\mathbb{F}_2^n$, the Boolean function ϕ_s: $y \in \mathbb{F}_2^m \mapsto \widetilde{f_y}(s)$ is bent.*

Recall that a way for constructing bent Boolean functions is, after identifying $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ with the Galois fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^m}$ respectively, to use the following Proposition given by Carlet ([31], section 6) and which is a consequence of Theorem 4.5.5. For completeness, we include the proof.

Proposition 4.5.6. *([31]) Let n and m be two positive integers. Let k be a Boolean function on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$. Define a Boolean function h on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by setting, for every (x, y, z, t) in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, $h(x, y, z, t) = k(\frac{x}{y}, \frac{z}{t})$.*

Assume the following conditions (1) and (2) are satisfied.

1. *For every $x \in \mathbb{F}_{2^n}$, the Boolean function $z \in \mathbb{F}_{2^m} \mapsto k(x, z)$ is balanced;*
2. *For every $z \in \mathbb{F}_{2^m}$, the Boolean function $x \in \mathbb{F}_{2^n} \mapsto k(x, z)$ is balanced.*

Then, the Boolean function h is bent.

Proof. Thanks to hypotheses (1) and (2), for every $(z, t) \in (\mathbb{F}_{2^m})^2$, the Boolean function $g_{z,t} : (x, y) \mapsto k(\frac{x}{y}, \frac{z}{t})$ belongs then to PS_{ap} class and thus is bent. Moreover, its dual $\widetilde{g_{z,t}}$ is defined by $\widetilde{g_{z,t}}(x, y) = k(\frac{y}{x}, \frac{z}{t})$. Therefore, the Boolean function $(z, t) \in (\mathbb{F}_{2^m})^2 \mapsto \widetilde{g_{z,t}}(x, y)$ belongs also to the PS_{ap} class for every (x, y) in $(\mathbb{F}_{2^m})^2$. We then conclude thanks to Theorem 4.5.5. □

The construction given by Proposition 4.5.6 can be straightforwardly extended to vectorial Boolean functions as follows.

Proposition 4.5.7. *([16]) Let n, m , r be three positive integers such that $r \leq n$ and $r \leq m$. Let K be a function from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^r}$ or to $\mathbb{F}_2^r$ such that*

1. *For every $x \in \mathbb{F}_{2^n}$, the function $y \in \mathbb{F}_{2^m} \mapsto K(x, y)$ is balanced,*
2. *For every $y \in \mathbb{F}_{2^m}$, the function $x \in \mathbb{F}_{2^n} \mapsto K(x, y)$ is balanced.*

Define the function H from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^r}$ by setting $H(x, y, z, t) = K(\frac{x}{y}, \frac{z}{t})$. Then H is a bent $(2n + 2m, r)$-function.

Proof. Apply Proposition 4.5.6 to each component function k_λ (where $\lambda \in \mathbb{F}_{2^r}$, $\lambda \neq 0$ or $\lambda \in \mathbb{F}_2^r \setminus \{0\}$) of the function K, that is the functions of the form $k_\lambda(x, y, z, t) = \mathrm{Tr}_1^r(\lambda K(\frac{x}{y}, \frac{z}{t}))$ or $\lambda \cdot K(\frac{x}{y}, \frac{z}{t})$ which is balanced (since a vectorial function is balanced if and only if all its component functions are balanced). □

Example 4.5.8. *Let ϕ and ϕ' be two balanced functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^n}$. Let F be a balanced function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$. Then, the function $K(x, y) := F(\phi(x) + \phi'(y))$ satisfies the conditions (1) and (2) of Proposition 4.5.7. Note that, in general, the corresponding bent function is not the direct sum (see definition below) of functions in x and y.*

3. Other primary constructions of bent vectorial functions:

The existence of a bent (n, r)-function is equivalent to the existence of an r-dimensional vectorspace of n-variable Boolean functions whose nonzero elements (the component functions of the vectorial function) are all bent. Let us give some examples of such construction:

• An example derived from the property of some codes: recall that, for given n and $r \leq n$, the binary Reed-Muller code $\mathcal{RM}(r, n)$ of order r and length 2^n consists of all n-variable Boolean functions of algebraic degree at most r and that the Kerdock code $\mathcal{K}(n)$ [98] of same length consists of the binary Reed-Muller code $\mathcal{RM}(1, n)$ of order 1 and length 2^n together with $2^{n-1} - 1$ cosets of $\mathcal{RM}(1, n)$ in the binary Reed-Muller code $\mathcal{RM}(2, n)$ of order 2 and length 2^n. The Boolean functions associated with these cosets are quadratic bent functions, with the property that the sum of any two of them is again a bent function. Consequently, any $(n, 2)$-function whose coordinate functions belong to two distinct cosets, among these $2^{n-1} - 1$ cosets, is a bent

vectorial function.

• Given a function F from $\mathbb{F}_{2^n}$ to itself, a nonzero element $a \in \mathbb{F}_{2^n}$ and an integer r dividing n, the (n,r)-function $x \in \mathbb{F}_{2^n} \mapsto \mathrm{Tr}_r^n(aF(x))$ is bent if and only if, for any nonzero $v \in \mathbb{F}_{2^r}$, the Boolean function $x \in \mathbb{F}_{2^n} \mapsto \mathrm{Tr}_1^n(avF(x))$ is bent.
Examples of constructions of such bent (n,r)-functions are given in [12] (with r strictly smaller than $n/2$). The authors obtain their results from some specific (n,n)-functions F (and under some assumptions on the nonzero element $a \in \mathbb{F}_{2^n}$ given in [12]):
-$F(x) = x^{2^i+1} + (x^{2^i} + x + 1)\,\mathrm{Tr}_1^n(x^{2^i+1})$, for $n \geq 6$ an even integer;
- $F(x) = \big(x + \mathrm{Tr}_3^n(x^{2(2^i+1)} + x^{4(2^i+1)}) + \mathrm{Tr}_1^n(x)\,\mathrm{Tr}_3^n(x^{2^i+1} + x^{2^{2i}(2^i+1)})\big)^{2^i+1}$, for n divisible by 6;
where i is a positive integer not divisible by $n/2$ and such that $n/\gcd(i,n)$ is even. The derived bent (n,r)-functions are CCZ-inequivalent to the quadratic (n,r)-functions $x \in \mathbb{F}_{2^n} \mapsto \mathrm{Tr}_r^n(vx^{2^i+1})$, $v \in \mathbb{F}_{2^r}$, $v \neq 0$.

• An example of bent $(n,n/2)$-function has been found by the first author in common with Leander. Such function is defined precisely, from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^{n/2}$, for n divisible by 2 but not by 4. The output of the function is of the form $(\mathrm{Tr}_1^n(\beta_1 w X^d), \cdots, \mathrm{Tr}_1^n(\beta_{n/2} w X^d)) \in \mathbb{F}_2^{n/2}$, $(X \in \mathbb{F}_{2^n})$; where d is a so-called Gold exponent: $d = 2^i + 1$ such that $\gcd(n,i) = 1$, where w is some element of $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$ and where $(\beta_1, \cdots, \beta_{n/2})$ is a basis of $\mathbb{F}_{2^{n/2}}$ over $\mathbb{F}_2$. More details concerning this construction can be found in [32].

4.5.2 Secondary constructions of bent vectorial functions

1. A Maiorana-McFarland-like construction:

In [27] is given the following secondary construction of bent Boolean functions: let r and s be two positive integers with the same parity and such that $r \leq s$, and let $n = r + s$; let ϕ be a function from $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$ and g a Boolean function on $\mathbb{F}_2^s$; let us assume that ϕ is balanced and, for every $a \in \mathbb{F}_2^r$, the set $\phi^{-1}(a)$ is an $(s-r)$-dimensional affine subspace of $\mathbb{F}_2^s$; let us assume additionally if $r < s$ that the restriction of g to $\phi^{-1}(a)$ (viewed as a Boolean function on $\mathbb{F}_2^{n-2r}$ via an affine isomorphism between $\phi^{-1}(a)$ and this vectorspace) is bent; then the function $f_{\phi,g}(x,y) = x \cdot \phi(y) + g(y)$, $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^s$, where "$\cdot$" is an inner product in $\mathbb{F}_2^r$, is bent on $\mathbb{F}_2^n$. This generalizes directly to vectorial functions:

Proposition 4.5.9. *([16]) Let r and s be two positive integers with the same parity and such that $r \leq \frac{s}{3}$. Let ψ be any (balanced) function from $\mathbb{F}_2^s$ to $\mathbb{F}_{2^r}$ such that, for every $a \in \mathbb{F}_{2^r}$, the set $\psi^{-1}(a)$ is an $(s-r)$-dimensional affine subspace of $\mathbb{F}_2^s$. Let H be any (s,r)-function whose restriction to $\psi^{-1}(a)$ (viewed as an $(s-r,r)$-function via an affine isomorphism between $\psi^{-1}(a)$ and $\mathbb{F}_2^{s-r}$) is bent for every $a \in \mathbb{F}_{2^r}$. Then, the function $F_{\psi,H}(x,y) = x\,\psi(y) + H(y)$, $x \in \mathbb{F}_{2^r}, y \in \mathbb{F}_2^s$, is a bent function from $\mathbb{F}_2^{r+s}$ to $\mathbb{F}_{2^r}$.*

Proof. Taking $x \cdot y = \mathrm{Tr}_1^r(xy)$ for inner product in $\mathbb{F}_{2^r}$, for every $v \in \mathbb{F}_{2^r}^*$, the function $\mathrm{Tr}_1^r(v\,F_{\psi,H}(x,y))$ is bent, according to the result of [27] recalled above, with $\phi(y) = v\,\psi(y)$ and $g(y) = \mathrm{Tr}_1^r(v\,H(y))$. The condition $r \leq \frac{s}{3}$, more restrictive than $r \leq s$, is meant so that $r \leq \frac{s-r}{2}$, which is necessary for allowing the restrictions of H to be bent. The condition on ψ being easily satisfied (this does not make ψ necessarily affine). Note that it is a simple matter to choose H. □

The direct sum of bent functions

It is well know that the direct sum $(x, y) \mapsto g(x) + h(y)$ of two bent Boolean functions f, g gives a bent Boolean function. This simple secondary construction can be directly adapted to vectorial functions. Indeed any bent (n, r)-function G and bent (m, r)-function H give a bent $(n + m, r)$-function F by setting, for $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$, $F(x, y) := G(x) + H(y)$.
2. An "indirect sum" of bent function construction:

The direct sum of bent Boolean functions is a particular case of a much more general construction introduced in [28], which involves 4 bent Boolean functions, and which has been recently called the indirect sum. The indirect sum does not seem generalizable into a secondary construction of bent vectorial functions involving 4 bent vectorial functions. But we show however below that it can be adapted to vectorial functions into a rather general construction. Let us first recall what is the indirect sum of bent Boolean functions. It is a particular case of the construction given by Theorem 4.5.5, which has the interest of automatically generating bent functions from bent functions, without that any extra condition be necessary (contrary to Theorem 4.5.5):

Proposition 4.5.10. *([28]) Let n and m be two even integers. Let f_1 and f_2, be two Boolean functions defined on $\mathbb{F}_2^n$, f_1' and f_2' be two Boolean functions defined on $\mathbb{F}_2^m$. Define the Boolean function h on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ by setting, for every $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$:*

$$h(x, y) = f_1(x) + f_1'(y) + (f_1(x) + f_2(x))(f_1'(y) + f_2'(y)).$$

If f_1, f_2, f_1' and f_2' are bent then, h is bent. Moreover, its dual $\widetilde{h}$ is obtained from $\widetilde{f_1}$, $\widetilde{f_2}$, $\widetilde{f_1'}$ and $\widetilde{f_2'}$ by the same formula as h is obtained from f_1, f_2, f_1' and f_2':

$$\widetilde{h}(x, y) = \widetilde{f_1}(x) + \widetilde{f_1'}(y) + (\widetilde{f_1}(x) + \widetilde{f_2}(x))(\widetilde{f_1'}(y) + \widetilde{f_2'}(y)).$$

This construction can be extended to vectorial Boolean functions as follows.

Proposition 4.5.11. *([16]) Let n, m and r be three positive integers such that n and m are even. Let F_1 and F_2 be two (n, r)-functions and $G = (g_1, \ldots, g_{r+1})$ be an $(m, r + 1)$-function. Define the function H from $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\mathbb{F}_2^r$ by setting, for every (x, y) in $\mathbb{F}_2^n \times \mathbb{F}_2^m$:*

$$H(x, y) = F_1(x) + G_1(y) + g_1(y)(F_1(x) + F_2(x))$$

where G_1 is the (m, r)-function $(g_2, \ldots, g_{r+1})$.

Assume that

1. *F_1 and F_2 are bent (this requires $r \leq \frac{n}{2}$);*
2. *For every λ in $\mathbb{F}_2^{r+1}$ different from $(1, 0, \ldots, 0)$, the component function $\lambda \cdot G$ is bent.*

Then H is a bent $(n + m, r)$-function.

Proof. Let $\delta \in \mathbb{F}_2^r \setminus \{0\}$. The component function $\delta \cdot H$ of H, that we denote by h_δ, has the form : $h_\delta(x, y) = \delta \cdot F_1(x) + \delta \cdot G_1(y) + g_1(y)(\delta \cdot F_1(x) + \delta \cdot F_2(x))$. This component function falls then in the scope of Proposition 4.5.10 if we take $f_1 = \delta \cdot F_1$, $f_2 = \delta \cdot F_2$, $f_1' = \delta \cdot G_1$ and $f_2' = g_1 + \delta \cdot G_1$. The bentness of h_δ is then a straightforward application of Proposition 4.5.10 since the assumptions (1) and (2) imply that f_1, f_2, f_1' and f_2' are bent. □

Remark 4.5.12. *The condition on G can be weakened. Indeed, let $G = (g_1, \ldots, g_{r+1})$ be an $(m, r + 1)$-function whose component functions $\lambda \cdot G$ are bent for every non zero $\lambda \neq \mu$ for some $\mu \in \mathbb{F}_2^{r+1} \setminus \{0\}$; let L be a linear automorphism of $\mathbb{F}_2^{r+1}$; set $G' = L \circ G$ then, for every $\lambda \in \mathbb{F}_2^{r+1} \setminus \{0\}$, we have: $\lambda \cdot G' = L^\star(\lambda) \cdot G$ for every $\lambda \in \mathbb{F}_2^{r+1} \setminus \{0\}$, where $L^\star$ denotes the adjoint operator of L. Therefore, one can choose L so that $L^\star(\mu) = (1, 0, \ldots, 0)$ and apply Proposition 4.5.11 to G'.*

Remark 4.5.13. *Obviously, condition (2) of Proposition 4.5.11 is satisfied by any bent $(m, r+1)$-function. The bentness of G is a strictly stronger hypothesis than hypothesis (2) in Proposition 4.5.11 (we shall see below an example of a non-bent function satisfying (2)) but it allows then to build many more bent functions H, since any function $G' := (g'_1, \ldots, g'_{r+1})$ affinely equivalent to G can be taken in Proposition 4.5.11 instead of G. The function g'_1 can in particular be taken equal to any of the $2^{r+1}-1$ component functions of G. These component functions are all distinct since G is bent. If $g_1 = g'_1$, the functions H corresponding to G and to G' may be affinely equivalent, but if $g_1 \neq g'_1$, they are not, in general. Hence, when applied to a bent function G, Proposition 4.5.11 can lead to $2^{r+1}-1$ affinely inequivalent functions H, given F_1, F_2 and G.*

Remark 4.5.14. *If g_1 is not constant, the algebraic degree of H is the maximum value between $\deg(g_1) + \deg(F_1 + F_2)$ and $\deg(G_1)$. In particular, H has algebraic degree $\frac{n+m}{2}$ (the optimum degree for a bent $(n+m, r)$-function) if and only if $\deg(F_1 + F_2) = \frac{n}{2}$ and $\deg(g_1) = \frac{m}{2}$ (which is optimal, since g_1 is the difference between two bent m-variable Boolean functions).*

We shall now investigate some non-bent functions G whose component functions are all bent except one and which will lead to corollaries of Proposition 4.5.11.

Example 4.5.15. *Let G' be any bent (m, r)-function. Let ℓ be an affine Boolean function on $\mathbb{F}_2^m$. Let G be the $(m, r+1)$-function defined as $G(y) = (\ell(y), G'(y))$. Then, all the component functions of G except its first coordinate function are bent.*

Using the particular choice stated in Example 4.6.5, one deduces the following corollary.

Corollary 4.5.16. *([16]) Let n, m and r be three positive integers such that n and m are even, $r \leq \frac{n}{2}$ and $r \leq \frac{m}{2}$. Let F_1 and F_2 be two bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^r$, G_1 a bent function from $\mathbb{F}_2^m$ to $\mathbb{F}_2^r$ and ℓ be an affine Boolean function on $\mathbb{F}_2^m$. Define the function H from $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\mathbb{F}_2^r$ by setting, for every $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$:*

$$H(x, y) = F_1(x) + G_1(y) + \ell(y)(F_1(x) + F_2(x))$$

Then H is a bent $(n+m, r)$-function.

This construction does not allow obtaining bent functions of maximal degree $\frac{n+m}{2}$ unless m equals 2. Let us give now another example of function G which has not this drawback.

Example 4.5.17. *Set $m = 2r$ and let us identify $\mathbb{F}_2^r$ with $\mathbb{F}_{2^r}$ and $\mathbb{F}_{2^m}$ with $\mathbb{F}_{2^r} \times \mathbb{F}_{2^r}$. Let us choose for G a function from $\mathbb{F}_{2^r} \times \mathbb{F}_{2^r}$ to $\mathbb{F}_2 \times \mathbb{F}_{2^r}$ of the form $G(y, z) = (\ell(y) + g(z), y\pi(z) + \Gamma(z))$ where π is a permutation of $\mathbb{F}_{2^r}$, Γ is any function from $\mathbb{F}_{2^r}$ to $\mathbb{F}_{2^r}$, ℓ is affine Boolean on $\mathbb{F}_{2^r}$ and g is any Boolean function on $\mathbb{F}_{2^r}$. Let $\lambda = (\eta, \mu) \in \mathbb{F}_2 \times \mathbb{F}_{2^r}$. For every $\mu \neq 0$ and $\eta \in \mathbb{F}_2$, the component function $\lambda \cdot G$ is by definition of the form $\lambda \cdot G(y, z) = \mathrm{Tr}_1^r(\mu y\pi(z) + \mu\Gamma(z)) + \eta\ell(y) + \eta g(z)$, for every (y, z) in $(\mathbb{F}_{2^r})^2$. Hence it belongs to the Maiorana-McFarland class of Boolean bent functions (see e.g. [31], Section 6).*

Using the particular choice stated in Example 4.5.17, one deduces the following corollary (where we identify $\mathbb{F}_2^s$ with the Galois Field $\mathbb{F}_{2^s}$).

Corollary 4.5.18. *([16]) Let n and r be two positive integers such that n is even and $r \leq \frac{n}{2}$. Let F_1 and F_2 be two bent functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$, g a Boolean function over $\mathbb{F}_{2^r}$, Γ a function from $\mathbb{F}_{2^r}$ to itself, π a permutation of $\mathbb{F}_{2^r}$ and ℓ an affine Boolean function over $\mathbb{F}_{2^r}$. Define the function H from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^r} \times \mathbb{F}_{2^r}$ to $\mathbb{F}_{2^r}$ by setting, for every $(x, y, z) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^r} \times \mathbb{F}_{2^r}$:*

$$H(x, y, z) = F_1(x) + y\pi(z) + \Gamma(z) + (\ell(y) + g(z))(F_1(x) + F_2(x))$$

Then H is a bent $(n + 2r, r)$-function.

3. Generalization of the indirect sum construction:

The indirect sum of Boolean functions was a consequence of Theorem 4.5.5. We shall see now that Theorem 4.5.5 leads to a construction of bent vectorial functions which is more general than that of Proposition 4.5.11. In this latter proposition, function H was equal to $F_1(x) + c_1$ (where $c_1 \in \mathbb{F}_2$) for some values of y and $F_2(x) + c_2$ (where $c_2 \in \mathbb{F}_2$) for the other values of y. This generalizes as follows.

Proposition 4.5.19. *([16]) Let n and m be two even integers and r, k two positive integers. Let $F_1, \cdots, F_k$ be (n,r)-functions and G an (m,r)-function. Let $\varphi_1, \ldots, \varphi_k$ be Boolean functions on $\mathbb{F}_2^m$ whose supports constitute a partition of $\mathbb{F}_2^m$. Let us define the vectorial Boolean function H from $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\mathbb{F}_2^r$ by setting, for every (x,y) in $\mathbb{F}_2^n \times \mathbb{F}_2^m$:*

$$H(x,y) = \sum_{i=1}^{k} \varphi_i(y) F_i(x) + G(y).$$

Let us assume that the following conditions (1) and (2) are satisfied:

1. *$F_1, \cdots, F_k$ and G are bent (this requires $r \leq \frac{n}{2}$ and $r \leq \frac{m}{2}$);*
2. *$\forall \lambda \in \mathbb{F}_2^r \setminus \{0\}, \forall \epsilon = (\epsilon_1, \cdots \epsilon_k) \in \mathbb{F}_2^k$,*
   the Boolean function $y \in \mathbb{F}_2^m \mapsto \sum_{j=1}^{k} \epsilon_j \varphi_j(y) + \lambda \cdot G(y)$ is bent.

Then H is a bent $(n+m,r)$-function.

Proof. Let $\lambda \in \mathbb{F}_2^r \setminus \{0\}$. The component function $\lambda \cdot H$ of H equals : $\sum_{i=1}^{k} \varphi_i(y)\ \lambda \cdot F_i(x) + \lambda \cdot G(y)$. The function $x \mapsto \lambda \cdot H(x,y)$ is bent for every y in $\mathbb{F}_2^m$ and its dual equals $\sum_{i=1}^{k} \varphi_i(y) \widetilde{\lambda \cdot F_i}(x) + \lambda \cdot G(y)$. Hence, applying condition (2) with $\epsilon_i = \widetilde{\lambda \cdot F_i}(x)$ proves that H is bent, according to Theorem 4.5.5. □

Remark 4.5.20. *Condition (2) of Proposition 4.5.19 implies in particular that for every $j \in \{1, \cdots, k\}$, the Boolean function defined over $\mathbb{F}_2^m$ by $h_j := \varphi_j + \lambda \cdot G$ is bent. Then $wt(h_j)$ has the form $2^{m-1} + \gamma_j 2^{\frac{m}{2}-1}$ with $\gamma_j = \pm 1$. The function $\lambda \cdot G$ is also bent then, $wt(\lambda \cdot G) = 2^{m-1} + \eta 2^{\frac{m}{2}-1}$ with $\eta = \pm 1$. On the other hand, we have $wt(h_j) = wt(\varphi_j) + wt(\lambda \cdot G) - 2wt(\varphi_j(\lambda \cdot G))$. Therefore, thanks to assumptions on φ_j, we have $\sum_{j=1}^{k} wt(h_j) = 2^m + (k-2)wt(\lambda \cdot G)$. Finally, $\sum_{j=1}^{k}(2^{m-1} + \gamma_j 2^{\frac{m}{2}-1}) = 2^m + (k-2)(2^{m-1} + \eta 2^{\frac{m}{2}-1})$ and then, $\sum_{j=1}^{k} \gamma_j = \eta(k-2)$.*

The following statement is an example of application of Proposition 4.5.19:

Corollary 4.5.21. *([16]) Let k, n and r be three positive integers such that n is even and $r \leq \frac{n}{2}$. Let $F_1, \cdots, F_k$ be bent (n,r)-functions, π a permutation of $\mathbb{F}_2^r$ and Γ any (r,r)-function. Let φ_1, $\ldots$, φ_k be any Boolean functions on $\mathbb{F}_2^r$ whose supports constitute a partition of $\mathbb{F}_2^r$. Define the function H from $\mathbb{F}_2^n \times \mathbb{F}_2^r \times \mathbb{F}_2^r$ to $\mathbb{F}_2^r$ by setting, for every $(x,y,z) \in \mathbb{F}_2^n \times \mathbb{F}_2^r \times \mathbb{F}_2^r$:*

$$H(x,y,z) = \sum_{i=1}^{k} \varphi_i(z) F_i(x) + y \cdot \pi(z) + \Gamma(z)$$

Then H is a bent $(n+2r,r)$-function.

Remark 4.5.22. *Corollary 4.5.21 can also be viewed as a generalization to vectorial functions of a secondary construction given in [35] for Boolean functions under the name of "extension of*

Maiorana-McFarland type" and which can be stated as follows: let π be a permutation on $\mathbb{F}_2^{n/2}$, g be a Boolean function on $\mathbb{F}_2^{n/2}$ and $f_{\pi,g}$ be a related Maiorana-McFarland's bent function that is, $f_{\pi,g}(x,y) = x\pi(y) + g(y)$, $(x,y) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$. Let $(h_y)_{y\in\mathbb{F}_2^{n/2}}$ be a collection of bent functions from $\mathbb{F}_2^m$ (for some even integer m) to $\mathbb{F}_2^{n/2}$. Then, the function $(x,y,z) \mapsto h_y(z) + f_{\pi,g}(x,y)$ defined from $\mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \times \mathbb{F}_2^m$ to $\mathbb{F}_2^{n/2}$, is a bent $(n+m, n/2)$-function.

4. Further generalization of the indirect sum construction:
Still more generally, Theorem 4.5.5 leads to a construction of vectorial functions as follows:

Proposition 4.5.23. *([16]) Let r and s be two positive even integers and m a positive integer such that $m \leq r/2$. Let H be a function from $\mathbb{F}_2^n = \mathbb{F}_2^r \times \mathbb{F}_2^s$ to $\mathbb{F}_2^m$. Assume that, for every $y \in \mathbb{F}_2^s$, the function $H_y : x \in \mathbb{F}_2^r \mapsto H(x,y)$ is a bent (r,m)-function. For every nonzero $v \in \mathbb{F}_2^m$ and every $a \in \mathbb{F}_2^r$ and $y \in \mathbb{F}_2^s$, let us denote by $f_{a,v}(y)$ the value at a of the dual of the Boolean function $v \cdot H_y$, that is, the binary value such that $\sum_{x\in\mathbb{F}_2^r}(-1)^{v\cdot H(x,y)+a\cdot x} = 2^{r/2}(-1)^{f_{a,v}(y)}$. Then H is bent if and only if, for every nonzero $v \in \mathbb{F}_2^m$ and every $a \in \mathbb{F}_2^r$, the Boolean function $f_{a,v}$ is bent.*

Proof. For every nonzero $v \in \mathbb{F}_2^m$ and every $a \in \mathbb{F}_2^r$ and $b \in \mathbb{F}_2^s$ we have:

$$\sum_{\substack{x\in\mathbb{F}_2^r\\ y\in\mathbb{F}_2^s}} (-1)^{v\cdot H(x,y)+a\cdot x+b\cdot y} = 2^{r/2} \sum_{y\in\mathbb{F}_2^s} (-1)^{f_{a,v}(y)+b\cdot y}.$$

□

Proposition 4.5.23 is very general and not very effective but an effective example can be obtained by choosing every H_y in the Maiorana-McFarland class: $H_y(x,x') = x\,\pi_y(x') + G_y(x')$, $x, x' \in \mathbb{F}_{2^{r/2}}$, where π_y is bijective for every $y \in \mathbb{F}_2^s$. We have then $f_{(a,a'),v}(y) = \mathrm{Tr}_1^{\frac{r}{2}}\left(a'\,\pi_y^{-1}\left(\frac{a}{v}\right) + v\,G_y\left(\pi_y^{-1}\left(\frac{a}{v}\right)\right)\right)$. Then H is bent if and only if, for every $v \in \mathbb{F}_{2^{r/2}}^*$ and every $a, a' \in \mathbb{F}_{2^{r/2}}$, the function $y \mapsto \mathrm{Tr}_1^{\frac{r}{2}}\left(a'\,\pi_y^{-1}(a) + v\,G_y(\pi_y^{-1}(a))\right)$ is bent on $\mathbb{F}_2^s$. A simple possibility for achieving this is for $s = r/2$ to choose π_y^{-1} such that, for every a, the function $y \mapsto \pi_y^{-1}(a)$ is an affine automorphism of $\mathbb{F}_{2^{r/2}}$ (*e.g.* $\pi_y^{-1}(a) = \pi_y(a) = a + y$) and to choose G_y such that, for every a, the function $y \mapsto G_y(a)$ is bent.

Remark 4.5.24. *The secondary constructions given in the present paper do not allow constructing a bent function whose number of output bits is strictly larger than the numbers of output bits of the functions used to build it. In particular, they do not allow constructing bent $(n, n/2)$-functions. We leave as an open problem such construction. Note that, if F is a bent (n,r)-function, then an affine subspace E of dimension strictly larger than $n/2$ of $\mathbb{F}_2^n$ cannot have an image by F included in an affine hyperplane of $\mathbb{F}_2^r$ since we know that an n-variable bent Boolean function cannot be constant on an affine subspace E of dimension strictly more than $n/2$ (see [24]) and if the image of E by F is included in an affine hyperplane of $\mathbb{F}_2^r$, then there exists $v \neq 0$ in $\mathbb{F}_2^r$ such that $v \cdot F$ is constant on E. This means that, in a secondary construction of a bent $(n, n/2)$-function F from two bent functions in smaller numbers of input variables and smaller numbers of output bits, at least one of the bent functions used to build F is inequivalent to any restriction of F (contrary to the constructions of Propositions 4.5.9, 4.5.19 and 4.5.23).*

4.6 Dillon's class H, class $\mathcal{H}$ and Niho bent functions

4.6.1 Classes H and $\mathcal{H}$ in bivariate form

In his thesis [87], Dillon introduces a third family of bent functions whose expression is given but whose bentness is achieved under some non-obvious condition (so the class is less explicit

than class $\mathcal{M}$ or class $\mathcal{PS}_{ap}$, but it happens to be more explicit than class $\mathcal{PS}$, the condition for H being easier to satisfy than for $\mathcal{PS}$, as we shall see). He defines these functions in bivariate form (but as we shall see, they can also be seen in univariate form). The functions of this family are defined as $f(x,y) = \mathrm{Tr}_1^m(y + xG(yx^{2^m-2}))$, with $x, y \in \mathbb{F}_{2^m}$ where G is a permutation of $\mathbb{F}_{2^m}$ such that $G(x) + x$ does not vanish and, for every $\beta \in \mathbb{F}_{2^m}^\star$, the function $G(x) + \beta x$ is two-to-one (i.e. the pre-image by this function of any element of $\mathbb{F}_{2^m}$ is either a pair or the empty set). He denotes this family of bent functions by H.
The condition that $G(x) + x$ does not vanish is required only for H to be an extension of $\mathcal{PS}$ but is not necessary for f to be bent. Similarly, the linear term $\mathrm{Tr}_1^m(y)$ can be taken off if we are only interested in the bentness of the function. We have then $f(x,y) = \begin{cases} \mathrm{Tr}_1^m\left(xG\left(\frac{y}{x}\right)\right) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$.
Note that the restriction of f to the vectorspaces $\{(x, ax)\,;\, x \in \mathbb{F}_{2^m}\}$ where $a \in \mathbb{F}_{2^m}$ are linear. More generally, any function whose restrictions to these vectorspaces are linear has the form:

$$g(x,y) = \begin{cases} \mathrm{Tr}_1^m\left(x\psi\left(\frac{y}{x}\right)\right) & \text{if } x \neq 0 \\ \mathrm{Tr}_1^m\left(\mu y\right) & \text{if } x = 0 \end{cases} \tag{4.2}$$

where $\mu \in \mathbb{F}_{2^m}$ and ψ is a mapping from $\mathbb{F}_{2^m}$ to itself. In the following proposition, we check (again, since this has been essentially done by Dillon) what is the necessary and sufficient condition on ψ and μ such that g is bent.

Proposition 4.6.1. *([44]) Let g be a Boolean function over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by* (4.2)*. Then g is bent if and only if, denoting $G(z) = \psi(z) + \mu z$, we have:*

$$G \text{ is a permutation on } \mathbb{F}_{2^m} \tag{4.3}$$

$$\text{For every } \beta \in \mathbb{F}_{2^m}^\star, \text{ the function } z \mapsto G(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m}. \tag{4.4}$$

Proof. For every $\alpha, \beta \in \mathbb{F}_{2^m}$, we have:

$$\begin{aligned}
\widehat{\chi_g}(\alpha,\beta) &= \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{g(x,y)+\mathrm{Tr}_1^m(\alpha x+\beta y)} \\
&= \sum_{x \in \mathbb{F}_{2^m}^\star, z \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m(x\psi(z)+\alpha x+\beta xz)} + \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m((\beta+\mu)y)} \\
&= \sum_{x \in \mathbb{F}_{2^m}, z \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m(x\psi(z)+\alpha x+\beta xz)} - 2^m + 2^m\delta_\mu(\beta) \\
&= 2^m \,\#\{z \in \mathbb{F}_{2^m} \,/\, \psi(z) + \alpha + \beta z = 0\} - 2^m + 2^m\delta_\mu(\beta).
\end{aligned}$$

We denote by $N_{\alpha,\beta}$ the cardinality of the set $\{z \in \mathbb{F}_{2^m} \,/\, \psi(z) + \alpha + \beta z = 0\}$.
Then we have $\widehat{\chi_g}(\alpha,\beta) = \begin{cases} 2^m N_{\alpha,\mu} & \text{if } \beta = \mu \\ 2^m N_{\alpha,\beta} - 2^m & \text{if } \beta \neq \mu \end{cases}$, and Conditions (4.3) and (4.4) are necessary and sufficient for g being bent. □

Definition 4.6.2. *We call $\mathcal{H}$ the extended class of H equal to the set of functions g defined by (4.2) and satisfying* (4.3) *and* (4.4) *(that is, satisfying* (4.4)*, since we shall see below that Condition* (4.4) *implies Condition* (4.3)*).*

Note that the function g defined by (4.2) satisfies $g(x,y)+\mathrm{Tr}_1^m(\mu y) = \begin{cases} \mathrm{Tr}_1^m\left(xG\left(\frac{y}{x}\right)\right) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$ and that changing $G(x)$ into $G(x)+\nu$ changes $g(x,y)$ into $g(x,y)+\mathrm{Tr}_1^m(\nu x)$. Hence, we can assume without loss of generality (up to the addition of a linear function) that $\mu = 0$ and $G(0) = 0$.

We consider now the duals of the functions in class $\mathcal{H}$. Under the conditions of Proposition 4.6.1:
- if $\beta = \mu$ then we have $\widehat{\chi_g}(\alpha,\beta) = 2^m$ and the equation $\psi(z)+\beta z = G(z) = \alpha$ has a solution;
- and if $\beta \neq \mu$ then we have $\widehat{\chi_g}(\alpha,\beta) = 2^m$ if and only if the equation $\psi(z)+\beta z = G(z)+(\beta+\mu)z = \alpha$ has solutions.

We deduce:

Proposition 4.6.3. *([44]) Let g be a bent function of the form (4.2) Then the dual function of g is defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as:*

$$\widetilde{g}(\alpha,\beta) = \begin{cases} 1 & \text{if the equation } \psi(z)+\beta z = G(z)+(\beta+\mu)z = \alpha \text{ has no solution in } \mathbb{F}_{2^m} \\ 0 & \text{otherwise} \end{cases}$$

Remark 4.6.4. *Since bent functions exist of the form (4.2), a natural question is: does there exist also semi-bent functions (see Chapter 8) of the same form* (4.2)*. Recall that a Boolean function is called semi-bent if its Walsh transform takes only the values* 0 *and* $\pm 2^{m+1}$*. Assume without loss of generality that $\mu = 0$ and that $G(0) = 0$. We remark that g is semi-bent if and only if $N_{\alpha,0} \in \{0,2\}$ and $N_{\alpha,\beta} \in \{1,3\}$ ($\beta \neq 0$). If $N_{\alpha,0} \in \{0,2\}$, $\widehat{\chi_g}(\alpha,0) \in \{0, 2^{m+1}\}$ and if $N_{\alpha,\beta} \in \{1,3\}$, $\widehat{\chi_g}(\alpha,\beta) \in \{0, 2^{m+1}\}$. This is impossible if $n > 2$ because of the Lemma 4.6.5 below. Therefore, there exists no semi-bent function of the form (4.2) for $n > 2$.*

Lemma 4.6.5. *Let g be a Boolean function. If the Walsh transform values of g are all non-negative, then g is affine.*

Proof. According to Parseval's relation $\sum_{\omega\in\mathbb{F}_2^n} \widehat{\chi_g}^2(\omega) = 2^{2n}$ and inverse Fourier transform formula $\sum_{\omega\in\mathbb{F}_2^n} \widehat{\chi_g}(\omega) = \pm 2^n$ (see e.g. [31]), we have: $\sum_{\omega\in\mathbb{F}_2^n} \widehat{\chi_g}^2(\omega) = (\sum_{\omega\in\mathbb{F}_2^n} \widehat{\chi_g}(\omega))^2$. This implies $\sum_{\omega\neq\omega'\in\mathbb{F}_2^n} \widehat{\chi_g}(\omega)\widehat{\chi_g}(\omega') = 0$ (relation valid for every Boolean function) and therefore, since the values of $\widehat{\chi_g}$ are non-negative: $\widehat{\chi_g}(\omega) = 0$ or $\widehat{\chi_g}(\omega') = 0$ for every $\omega \neq \omega'$. The Walsh transform of g takes therefore non-zero value at exactly one point and it is well-known that g is then affine (that is, has algebraic degree at most 1). □

A first infinite class of functions in $\mathcal{H}$

The Frobenius map $z \mapsto G(z) = z^2$ gives an example of functions G, which leads to a function in the class $\mathcal{H}$: $g(x,y) = \mathrm{Tr}_1^m(y^2 x^{2^m-2})$. More generally, one can get functions in the class $\mathcal{H}$ by considering the maps $z \mapsto G(z) = z^{2^i}$ where i is co-prime with m, since the equation $z^{2^i}+\beta z = \alpha$ is equivalent, denoting $\gamma = \beta^{\frac{1}{2^i-1}}$, to $\left(\frac{z}{\gamma}\right)^{2^i} + \frac{z}{\gamma} = \frac{\alpha}{\gamma^{2^i}}$. As observed by Dillon, the related bent functions are in the completed Maiorana-MacFarland class; indeed, denoting $j = m-i$, we have then $g(x,y) = \mathrm{Tr}_1^m(x\,(yx^{2^m-2})^{2^i}) = \mathrm{Tr}_1^m(x^{2^j} yx^{2^m-2}) = \mathrm{Tr}_1^m(yx^{2^j-1})$.

Stability of functions G

In the following, we study the stability of functions G satisfying Conditions (4.3) and (4.4). Note that Condition (4.4) is equivalent to saying that for every $\beta \in \mathbb{F}_{2^m}^\star$, the function $z \mapsto \beta G(z)+z$ is 2-to-1. Let G be a function satisfying Conditions (4.3) and (4.4). Then

1. the function $z \mapsto G^{-1}(z)$ satisfies Conditions (4.3) and (4.4), since denoting $G^{-1}(z)$ by z', the equation $G^{-1}(z) + \beta z = \alpha$ is equivalent to $G(z') + \frac{1}{\beta} z' = \frac{\alpha}{\beta}$.

2. the function $z \mapsto G'(z) := (L^{-1} \circ G \circ L)(z)$ where $L(z) = z^{2^j}$ is a field automorphism of $\mathbb{F}_{2^m}$, that is $G'(z) = (G(z^{2^j}))^{2^{m-j}}$, satisfies Conditions (4.3) and (4.4).

3. the function $z \mapsto G'(z) := \lambda G(z) + \lambda'$ with $\lambda \neq 0$ satisfies Conditions (4.3) and (4.4).

4. the function $z \mapsto G'(z) := G(\lambda z + \lambda')$ with $\lambda \neq 0$ satisfies Conditions (4.3) and (4.4).

5. the function $z \mapsto G'(z) := zG(z^{2^m-2})$ if $G(0) = 0$ and more generally the function $z \mapsto G'(z) := zG(z^{2^m-2}) + zG(0)$ for any value of $G(0)$ satisfies Conditions (4.3) and (4.4). Indeed (restricting ourself without loss of generality to the case $G(0) = 0$ - by replacing G by $G + G(0)$ - and still assuming that $\beta \neq 0$), if $\alpha \neq 0$ then $zG(z^{2^m-2}) = \alpha$ is equivalent to $G(z^{2^m-2}) = \alpha z^{2^m-2}$ which has one solution since $G(z) + \alpha z = 0$ has two solutions and $z = 0$ is one of them, and the equation $zG(z^{2^m-2}) + \beta z = \alpha$ is equivalent to $G(z^{2^m-2}) + \alpha z^{2^m-2} = \beta$ and has therefore 0 or 2 solutions; and if $\alpha = 0$ then $zG(z^{2^m-2}) = \alpha = 0$ is equivalent to $z = 0$ and the equation $zG(z^{2^m-2}) + \beta z = \alpha = 0$ is equivalent to $z = 0$ or $G(z^{2^m-2}) = \beta$ which has one (nonzero) solution.

Note that transformations (2) to (5) translated in terms of the associated bent functions $g(x, y) = \mathrm{Tr}_1^m \left(xG\left(\frac{y}{x}\right)\right)$ (with the convention $\frac{1}{0} = 0$) result in particular cases of EA-equivalence, since transformation (2) corresponds to applying the same field automorphism to x and y; transformations (3) and (4) correspond to multiplying x and/or y by constants in $g(x, y)$ and to adding linear functions to g; and transformation (5) corresponds when $G(0) = 0$ to swaping x and y in $g(x, y)$. On the contrary, the bent functions related by transformation (1) are not EA-equivalent, in general. We shall say that two functions G are *o-equivalent* (the reason why we choose such term will come below) if one can be obtained from the other by a sequence of the transformations $G \mapsto G'$ above. This gives a notion of equivalence of functions in class $\mathcal{H}$ which is not a sub-equivalence of the EA-equivalence of bent functions and is not a super-equivalence either.
Note that the general $\mathbb{F}_{2^m}$-linear equivalence between the corresponding bent functions (when one equals the other composed on the right by an $\mathbb{F}_{2^m}$-linear automorphism over $\mathbb{F}_{2^n}$) is included in this notion of o-equivalence: applying to the function $g(x, y) = \mathrm{Tr}_1^m \left(xG\left(\frac{y}{x}\right)\right)$ the transformation $(x, y) \mapsto (ax + by, cx + dy)$, where $a, b, c, d \in \mathbb{F}_{2^m}$ are such that $ad \neq bc$, gives the function $g'(x, y)$ equal, if $x \neq 0$, to $\mathrm{Tr}_1^m \left((ax + by)G\left(\frac{cx+dy}{ax+by}\right)\right) = \mathrm{Tr}_1^m \left(x(a + bz)G\left(\frac{c+dz}{a+bz}\right)\right)$, where $z = \frac{y}{x}$ (and still assuming the convention $\frac{1}{0} = 0$) and if $x = 0$ to $\mathrm{Tr}_1^m \left(byG\left(\frac{d}{b}\right)\right)$. This corresponds to the transformation

$$G'(z) = (a + bz)\, G\left(\frac{c + dz}{a + bz}\right) + bz\, G\left(\frac{d}{b}\right). \tag{4.5}$$

If $b = 0$, this transformation reduces to $G'(z) = a\, G\left(\frac{c+dz}{a}\right)$ (with $a \neq 0$ and $d \neq 0$ since $ad \neq bc$) and can be obtained by applying transformations (3) and (4), and if $b \neq 0$, then it corresponds to applying (3), (4) and (5).
Note that, conversely, we obtain transformation (3) with $\lambda' = 0$ by choosing $(a, b, c, d) = (\lambda, 0, 0, \lambda)$, and transformations (4) and (5) by choosing $(a, b, c, d) = (1, 0, \lambda', \lambda)$ and $(0, 1, 1, 0)$.

4.6.2 Class $\mathcal{H}$ in univariate form: Niho bent functions

We identify now $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with $\mathbb{F}_{2^n}$ by considering a basis (u, v) of the $\mathbb{F}_{2^m}$-vector space $\mathbb{F}_{2^n}$ and identifying $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with:

$$t = xu + yv.$$

Then the vectorspaces $\{(x, ax)\,;\, x \in \mathbb{F}_{2^m}\}$ where $a \in \mathbb{F}_{2^m}$ and $\{(0, y)\,;\, y \in \mathbb{F}_{2^m}\}$ become the $2^m + 1$ multiplicative cosets of $\mathbb{F}_{2^m}^\star$ in $\mathbb{F}_{2^n}^\star$, added with 0. These cosets can be written $\omega\mathbb{F}_{2^m}^\star$ where ω ranges over the multiplicative subgroup U of $\mathbb{F}_{2^n}^\star$ of order $2^m + 1$, if we want to have a unique representation of each of them. And if we allow repetition, they are the cosets $\omega\mathbb{F}_{2^m}^\star$ where $\omega \in \mathbb{F}_{2^n}^\star$. The necessary and sufficient condition for a bent function to belong to class $\mathcal{H}$ is then that its restriction to each vectorspace $\omega\mathbb{F}_{2^m}$, $\omega \in \mathbb{F}_{2^n}^\star$, is linear.

Lemma 4.6.6. *([44]) Let f be a Boolean function over $\mathbb{F}_{2^n}$ and $f(t) = \sum_{i=0}^{2^n-1} a_i t^i$ its univariate representation. Then the restrictions of f to the vectorspaces $\omega\mathbb{F}_{2^m}$, $\omega \in \mathbb{F}_{2^n}^\star$, are all linear if and only if the only exponents i such that $a_i \neq 0$ are congruent with powers of 2 modulo $2^m - 1$.*

Proof. The condition is clearly sufficient. Let us show that it is also necessary. Clearly, we must have $a_0 = 0$. Moreover, for every $\omega \in \mathbb{F}_{2^n}^\star$, the restriction of f to $\omega\mathbb{F}_{2^m}$ being linear, there exists $\lambda_\omega \in \mathbb{F}_{2^m}$ such that $f(\omega x) = \sum_{i=1}^{2^n-1} a_i \omega^i x^{i[\mathrm{mod}\ 2^m-1]}) = \mathrm{Tr}_1^m(\lambda_\omega x)$ for every $x \in \mathbb{F}_{2^m}^\star$. By uniqueness of the univariate representation of a Boolean function over $\mathbb{F}_{2^m}$ (here, a function of x), we deduce that, for every $k \in \{0, \ldots, 2^m - 2\}$ different from a power of 2, we have $\sum_{\substack{1 \le i \le 2^n-1 \\ i \equiv k \ [\mathrm{mod}\ 2^m-1]}} a_i \omega^i = 0$. This completes the proof, by uniqueness of the univariate representation of a function from $\mathbb{F}_{2^n}$ to itself (here, a function of ω). □

Note that this result extends to any function f from $\mathbb{F}_{2^n}$ to itself.
Recall that bent functions whose restrictions to the vectorspaces $\omega\mathbb{F}_{2^m}$ are all linear have already been investigated in [93] and [160]. Since the exponents congruent with powers of 2 modulo $2^m - 1$ are called Niho exponents, we shall call these functions *Niho bent functions*. We have seen in Section 4.4.2 yet five examples of infinite classes of Niho bent functions are known up to affine equivalence or more exactly, four examples since one of the classes is the generalization of one of the others.

4.7 A natural extension of class $\mathcal{H}$

Since class $\mathcal{H}$ is the set of bent functions whose restrictions to the $\omega\mathbb{F}_{2^m}$'s are linear, a natural extension to consider is the set of those bent functions whose restrictions to the $\omega\mathbb{F}_{2^m}^\star$'s are affine. Clearly, such functions are the sums of an element of class $\mathcal{H}$ and of a function which is constant on each $\omega\mathbb{F}_{2^m}^\star$ (note that, since bent functions have algebraic degree at most m, we can assume this function has even Hamming weight, and therefore has the form $\sum_{\omega \in S} 1_{\omega\mathbb{F}_{2^m}}$, where $1_{\omega\mathbb{F}_{2^m}}$ is the indicator of $\omega\mathbb{F}_{2^m}$).

Proposition 4.7.1. *([44]) Let h be an element of $\mathcal{H}$ (that is, a Boolean function whose restriction to every $\omega\mathbb{F}_{2^m}$, $\omega \in \mathbb{F}_{2^m}^\star$, is linear). Let S be any subset of U (the multiplicative subgroup of $\mathbb{F}_{2^n}^\star$ of order $2^m + 1$) and let $g = \sum_{\omega \in S} 1_{\omega\mathbb{F}_{2^m}}$. Then $g + h$ is bent if and only if g is constant and h is bent, or g is bent and h is linear or S equals a singleton $\{\omega_0\}$ or its complement and h is Niho bent.*

Proof. We may without loss of generality assume that $g(0) = 0$, that is, S has even size (up to replacing g by $g + 1$). As shown in [45], denoting then by g_ω the value of g on $\omega\mathbb{F}_{2^m}^\star$, we have:

$$\forall c \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{g+h}}(c) = 1 - \sum_{\omega \in U} \chi(g_\omega) + 2^m \sum_{\omega \in I(c)} \chi(g_\omega), \tag{4.6}$$

where $I(c) = \{\omega \in U \mid \forall t \in \omega\mathbb{F}_{2^m},\ h(t) = \mathrm{Tr}_1^n(ct)\}$

$$\text{and} \quad \widehat{\chi_h}(c) = 2^m(\#I(c) - 1). \tag{4.7}$$

According to (8.15), $g+h$ can be bent only if $1-\sum_{\omega\in U}\chi(g_\omega) \equiv 0 \pmod{2^m}$ that is, $\sum_{\omega\in U}\chi(g_\omega) = 1 + \epsilon 2^m$ with $\epsilon \in \{0, \pm 1\}$.
If $\epsilon = 1$, then $g = 0$.
If $\epsilon = 0$, then g is bent (it belongs to the PS_{ap} class) and $g + h$ is bent if and only if, for every c, we have $\sum_{\omega\in I(c)}\chi(g_\omega) \in \{-1, 1\}$. Necessarily $\#I(c)$ must then be odd, and according to (8.16), $\widehat{\chi_h}(c)$ is then non-negative. According to Lemma 4.6.5, h is then linear. Conversely, if g is bent and h is linear then $g + h$ is bent.
If $\epsilon = -1$, then $g_\omega = 0$ for a single ω, that is, $g = 1_{\omega_0\,\mathbb{F}_{2^m}} + 1$. We know from [24] that if a bent function f is affine on an m-dimensional affine space E then $f + 1_E$ is bent too. Then taking $E = \omega_0\,\mathbb{F}_{2^m}$, we see that $g + h$ is bent if and only if h is Niho bent (indeed, the restrictions of h and $g + h$ to $\omega_0\,\mathbb{F}_{2^m}$ are affine). □

Remark 4.7.2. *We can see that the corresponding bent functions $g + h$ are not really new: they are equal to "known" bent functions added with affine functions.*

4.8 On the duals of bent functions via Niho exponents

In the following, we are interested to compute the dual of bent functions in the class$\mathcal{H}$.

4.8.1 On the duals of the known binomial bent functions via Niho exponents

It was left open in [93] to determine if the duals of the functions introduced there are affinely equivalent to these Niho bent functions. In the next proposition, we study how the mapping G related to the functions in the second class satisfies Conditions (4.3) and (4.4). We subsequently study the duals of these functions and give an answer to this question.

We first calculate the polynomial $G(z)$ related to a generic Niho function $f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \sum_{i\in I}\mathrm{Tr}_1^n(b_i t^{(2^m-1)s_i+1})$ where $a \in \mathbb{F}_{2^m}$ and $b_i \in \mathbb{F}_{2^n}$ and where the s_i's are elements of the residue class ring $\mathbb{Z}/(2^m + 1)\mathbb{Z}$. Note that some of the s_i's can be taken equal to inverses in $(\mathbb{Z}/(2^m + 1)\mathbb{Z})^\star$ (this is the case in [93]), and that we can take them different from $1/2$ since the term corresponding to $s_i = 1/2$ appears as $\mathrm{Tr}_1^m(at^{2^m+1})$. Decomposing $t = ux + vy$ where (u, v) is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$ and denoting $z = y/x$, we have then:
- for $x \neq 0$, $f(t) = \mathrm{Tr}_1^m\left(x\left(a^{\frac{1}{2}}(u + vz)^{\frac{2^m+1}{2}} + \sum_{i\in I}\mathrm{Tr}_m^n(b_i(u + vz)^{(2^m-1)s_i+1})\right)\right)$;
- and for $x = 0$, $f(t) = \mathrm{Tr}_1^m\left(y\left(a^{\frac{1}{2}}v^{\frac{2^m+1}{2}} + \sum_{i\in I}\mathrm{Tr}_m^n(b_i v^{(2^m-1)s_i+1})\right)\right)$.

Hence we have (see Section 4.6.1) $\psi(z) = a^{\frac{1}{2}}(u + vz)^{\frac{2^m+1}{2}} + \sum_{i\in I}\mathrm{Tr}_m^n(b_i(u + vz)^{(2^m-1)s_i+1})$ and

$\mu = a^{\frac{1}{2}} v^{\frac{2^m+1}{2}} + \sum_{i\in I} \mathrm{Tr}_m^n(b_i v^{(2^m-1)s_i+1})$. Then we have:

$$G(z) = a^{\frac{1}{2}} \left((u+vz)^{\frac{2^m+1}{2}} + (vz)^{\frac{2^m+1}{2}} \right) + \sum_{i\in I} \mathrm{Tr}_m^n \left(b_i \left[(u+vz)^{(2^m-1)s_i+1} + (vz)^{(2^m-1)s_i+1} \right] \right). \tag{4.8}$$

Proposition 4.8.1. *([44]) Let f be defined as*

$$\forall t \in \mathbb{F}_{2^n}, \quad f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)\frac{1}{4}+1}) \tag{4.9}$$

with m odd, $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{2^n}^\star$. Let (u,v) be a basis of $\mathbb{F}_{2^n}$ as two dimensional vectorspace over $\mathbb{F}_{2^m}$. The restriction of f to $v\mathbb{F}_{2^m}$ equals $\mathrm{Tr}_1^m(\mu y)$ with $\mu = a^{1/2}v^{(2^m+1)/2} + \mathrm{Tr}_m^n(bv^{(2^m-1)\frac{1}{4}+1})$. The mapping G such that $G(z) = \psi(z) + \mu z$ and

$$f(ux+vy) = \begin{cases} \mathrm{Tr}_1^m\left(x\psi\left(\frac{y}{x}\right)\right) & \text{if } x \neq 0 \\ \mathrm{Tr}_1^m\left(()\,\mu y\right) & \text{if } x = 0 \end{cases}$$

can be characterised by

$$\begin{aligned} G^4(z) = {} & a^2 u^{2(2^m+1)} + \mathrm{Tr}_m^n(b^4 u^{2^m+3}) \\ & + \mathrm{Tr}_m^n(uv^{2^m}) \Big(\mathrm{Tr}_m^n(b^4u^2)z + [a^2\,\mathrm{Tr}_m^n(uv^{2^m}) + \mathrm{Tr}_m^n(b^4uv)]z^2 + \mathrm{Tr}_m^n(b^4v^2)z^3 \Big) \end{aligned}$$

Proof. According to (4.8), we have:

$$G^4(z) = a^2(u+vz)^{2(2^m+1)} + a^2v^{2(2^m+1)}z^4 + \mathrm{Tr}_m^n(b^4(u+vz)^{2^m+3}) + \mathrm{Tr}_m^n(b^4v^{2^m+3}z^4).$$

Note now that

$$(A+B)^{2^m+1} = A^{2^m+1} + B^{2^m+1} + \mathrm{Tr}_m^n(AB^{2^m}) \tag{4.10}$$

and

$$\begin{aligned} (A+B)^{2^m+3} &= (A+B)^{2^m+1}(A+B)^2 \\ &= \left(A^{2^m+1} + B^{2^m+1} + \mathrm{Tr}_m^n(AB^{2^m}) \right)(A^2+B^2) \\ &= A^{2^m+3} + B^{2^m+3} + A^{2^m+1}B^2 + B^{2^m+1}A^2 + \mathrm{Tr}_m^n(AB^{2^m})(A^2+B^2) \\ &= A^{2^m+3} + B^{2^m+3} + AB(A^{2^m}B + B^{2^m}A) + \mathrm{Tr}_m^n(AB^{2^m})(A^2+B^2) \\ &= A^{2^m+3} + B^{2^m+3} + \mathrm{Tr}_m^n(AB^{2^m})(A^2+B^2+AB). \end{aligned}$$

Therefore,

$$\begin{aligned} G^4(z) = {} & a^2 u^{2(2^m+1)} + \mathrm{Tr}_m^n(b^4 u^{2^m+3}) \\ & + \mathrm{Tr}_m^n(uv^{2^m}) \left(\mathrm{Tr}_m^n(b^4u^2)z + [a^2\,\mathrm{Tr}_m^n(uv^{2^m}) + \mathrm{Tr}_m^n(b^4uv)]z^2 + \mathrm{Tr}_m^n(b^4v^2)z^3 \right). \end{aligned}$$

□

We are now going to exhibit under which conditions on a and b the function satisfies conditions (4.3) and (4.4).

Note now that we can suppose without loss of generality that $\mathrm{Tr}_m^n(uv^{2^m}) = 1$. First of all, one has that $\mathrm{Tr}_m^n(uv^{2^m}) \neq 0$. Otherwise $u^{2^m-1}v^{1-2^m} = 1$ yielding $u/v \in \mathbb{F}_{2^m}$ contradicting the fact that (u,v) is a basis of $\mathbb{F}_{2^n}$ as two dimensional vectorspace over $\mathbb{F}_{2^m}$. Denoting by G'

the function obtained by replacing the basis (u, v) by $(u', v') = \left(\frac{u}{\mathrm{Tr}_m^n(uv^{2^m})^{\frac{1}{2}}}, \frac{v}{\mathrm{Tr}_m^n(uv^{2^m})^{\frac{1}{2}}}\right)$, we have the relation $G'(z) = \frac{G(z)}{\mathrm{Tr}_m^n(uv^{2^m})^{\frac{1}{2}}}$. Now, clearly, G satisfies conditions (4.3) and (4.4) if and only if G' satisfies conditions (4.3) and (4.4) and this allows us to restrict ourselves to the case $\mathrm{Tr}_m^n(uv^{2^m}) = 1$.

Proposition 4.8.2. *([44]) Let (u, v) be a basis of $\mathbb{F}_{2^n}$ as two dimensional vector space over $\mathbb{F}_{2^m}$ such that $\mathrm{Tr}_m^n(uv^{2^m}) = 1$. The corresponding function G of Proposition 4.8.1 is a permutation if and only if $b^{2^m+1} = a$. Furthermore, if $b^{2^m+1} = a$, there exists $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_{2^m}$ such that $\lambda_1 + \lambda_2 G(z + \lambda_3) = z^{\frac{1}{4}}$ for every $z \in \mathbb{F}_{2^m}$ or $\lambda_1 + \lambda_2 G(z + \lambda_3) = z^{\frac{3}{4}}$ for every $z \in \mathbb{F}_{2^m}$.*

Proof. The function G given by Proposition 4.8.1 is defined as

$$G(z) = A + Bz^{\frac{1}{4}} + Cz^{\frac{1}{2}} + Dz^{\frac{3}{4}}$$

with

$$\begin{aligned} A &= a^{1/2}u^{(2^m+1)/2} + \mathrm{Tr}_m^n(bu^{(2^m-1)\frac{1}{4}+1}) \\ B &= \mathrm{Tr}_m^n(bu^{\frac{1}{2}}) \\ C &= a^{1/2} + \mathrm{Tr}_m^n(bu^{\frac{1}{4}}v^{\frac{1}{4}}) \\ D &= \mathrm{Tr}_m^n(bv^{\frac{1}{2}}). \end{aligned}$$

For $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_{2^m}^3$ with $\lambda_2 \neq 0$,

$$\begin{aligned} \lambda_1 + \lambda_2 G(z + \lambda_3) = \lambda_1 &+ \lambda_2(A + B\lambda_3^{1/4} + C\lambda_3^{1/2} + D\lambda_3^{3/4}) \\ &+ \lambda_2((B + D\lambda_3^{1/2})z^{\frac{1}{4}} + (C + D\lambda_3^{1/4})z^{\frac{1}{2}} + Dz^{\frac{3}{4}}). \end{aligned}$$

Now, note that given a function $f \in \mathbb{F}_{2^n}[x]$, the *normalized form* of f is f' such that $f'(0) = 0$, the degree d of f' is not divisible by the characteristic of $\mathbb{F}_{2^n}$ that is, 2 and the coefficient of x^{d-1} is 0. The only permutations of degree at most three and in normalized form are $z \mapsto z^i$ with $i \in \{1, 2, 3\}$ (see [166], page 352). Therefore G is a permutation if and only if there exists $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_{2^m}^3$ such that $\lambda_1 + \lambda_2 G(z + \lambda_3) = z^{\frac{i}{4}}$ with $i \in \{1, 2, 3\}$, that is, there exists $\lambda_3 \in \mathbb{F}_{2^m}$ such that:

- for $i = 1$: $D = C = 0$ and $B \neq 0$;
- for $i = 2$: $D = B = 0$ and $C \neq 0$;
- for $i = 3$: $B + D\lambda_3^{1/2} = C + D\lambda_3^{1/4} = 0$ and $D \neq 0$.

In the two first cases, we have $D = 0$, that is $bv^{1/2} \in \mathbb{F}_{2^m}$. Then B cannot be equal to 0 otherwise $u/v \in \mathbb{F}_{2^m}$ contradicting the fact that (u, v) is a basis of $\mathbb{F}_{2^n}$ as two dimensional vector space over $\mathbb{F}_{2^m}$. Hence $i = 2$ is impossible. We characterize now the case $i = 1$. we have:

$$\begin{aligned} C = 0 &\iff a^{1/2} = \mathrm{Tr}_m^n(bu^{\frac{1}{4}}v^{\frac{1}{4}}) \\ &\iff a^{(2^m+1)/2} = b^{2^m+1}v^{(2^m+1)/2}\left(\mathrm{Tr}_m^n(u^{\frac{1}{4}}v^{-\frac{1}{4}})\right)^{2^m+1} \end{aligned}$$

We have used the fact that $z \mapsto z^{2^m+1}$ is a permutation of $\mathbb{F}_{2^m}$ since $\gcd(2^m + 1, 2^m - 1) = 1$ and that $bv^{1/2} \in \mathbb{F}_{2^m}$. Note then that

$$v^{(2^m+1)/2}\left(\mathrm{Tr}_m^n(u^{\frac{1}{4}}v^{-\frac{1}{4}})\right)^{2^m+1} = \left(v^2\,\mathrm{Tr}_m^n(uv^{-1})\right)^{(2^m+1)/4}$$

Now,

$$\begin{aligned} v^2 \operatorname{Tr}_m^n(uv^{-1}) &= v^2(uv^{-1} + u^{2^m} v^{-2^m}) \\ &= uv + u^{2^m} v^{2-2^m} \end{aligned}$$

Using (4.10) with $A = uv$ and $B = u^{2^m} v^{2-2^m}$ and noting that

$$\begin{aligned} B^{2^m+1} &= u^{2^m(2^m+1)} v^{(2-2^m)(2^m+1)} \\ &= u^{1+2^m} v^{1+2^m} = A^{2^m+1} \end{aligned}$$

and

$$\begin{aligned} AB^{2^m} &= uv \times \left(u^{2^m} v^{2-2^m}\right)^{2^m} \\ &= uv \times uv^{2^{m+1}-1} \\ &= u^2 v^{2^{m+1}} \\ &= \left(uv^{2^m}\right)^2 \end{aligned}$$

We have:

$$\begin{aligned} \left(v^2 \operatorname{Tr}_m^n(uv^{-1})\right)^{(2^m+1)} &= \operatorname{Tr}_m^n\left(\left(uv^{2^m}\right)^2\right) \\ &= \operatorname{Tr}_m^n(uv^{2^m})^2 \\ &= 1. \end{aligned}$$

Thus, since $a \in \mathbb{F}_{2^m}$, $a^{2^m} = a$ and therefore $a^{(2^m+1)/2} = a$, we have that

$$D = C + D\lambda_3^{1/4} = 0 \iff a = b^{2^m+1}.$$

We study now the case $i = 3$. We have $D \neq 0$, that is, $bv^{\frac{1}{2}} \notin \mathbb{F}_{2^m}$. Then,

$$\begin{aligned} \exists \lambda_3 \in \mathbb{F}_{2^m},\, B + D\lambda_3^{1/2} = C + D\lambda_3^{1/4} = 0 &\iff \exists \lambda_3 \in \mathbb{F}_{2^m},\, \frac{B}{D} = \lambda_3^{1/2} \text{ and } \frac{C}{D} = \lambda_3^{1/4} \\ &\iff \frac{B}{D} = \frac{C^2}{D^2} \\ &\iff BD = C^2. \end{aligned}$$

Now

$$BD = C^2 \iff \operatorname{Tr}_m^n(bu^{1/2}) \operatorname{Tr}_m^n(bv^{1/2}) = a + \operatorname{Tr}_m^n(b^2 u^{\frac{1}{2}} v^{\frac{1}{2}}).$$

Note now that

$$\begin{aligned} \operatorname{Tr}_m^n(X) \operatorname{Tr}_m^n(Y) &= (X + X^{2^m})(Y + Y^{2^m}) \\ &= XY + X^{2^m} Y^{2^m} + X^{2^m} Y + XY^{2^m} \\ &= \operatorname{Tr}_m^n(XY) + \operatorname{Tr}_m^n(XY^{2^m}). \end{aligned}$$

Applying the above equality with $X = bu^{1/2}$ and $Y = bv^{1/2}$, we get that

$$\begin{aligned}\mathrm{Tr}_m^n(bu^{1/2})\,\mathrm{Tr}_m^n(bv^{1/2}) &= \mathrm{Tr}_m^n\left((bu^{1/2})(bv^{1/2})\right) + \mathrm{Tr}_m^n\left((bu^{1/2})(bv^{1/2})^{2^m}\right)\\ &= \mathrm{Tr}_m^n\left(b^2u^{1/2}v^{1/2}\right) + \mathrm{Tr}_m^n\left(b^{2^m+1}\left(uv^{2^m}\right)^{1/2}\right)\\ &= \mathrm{Tr}_m^n\left(b^2u^{1/2}v^{1/2}\right) + b^{2^m+1}\,\mathrm{Tr}_m^n\left(uv^{2^m}\right)^{1/2}\\ &= \mathrm{Tr}_m^n\left(b^2u^{1/2}v^{1/2}\right) + b^{2^m+1}\end{aligned}$$

since $b^{2^m+1} \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_m^n\left(uv^{2^m}\right) = 1$. Therefore,

$$BD = C^2 \iff b^{2^m+1} = a.$$

that is,

$$\exists \lambda_3 \in \mathbb{F}_{2^m},\ B + D\lambda_3^{1/2} = C + D\lambda_3^{1/4} = 0 \iff b^{2^m+1} = a.$$

□

Lemma 4.8.3. *([44]) Let m be a positive odd integer. The permutation $\phi_i : z \mapsto z^{\frac{i}{4}}$ satisfies condition 4.4 for every $i \in \{1, 3\}$.*

Proof. For every $b \in \mathbb{F}_{2^m}^\star$, the kernel of the linear map $z \in \mathbb{F}_{2^m} \mapsto \phi_1(z) + bz$ is of dimension 1 over $\mathbb{F}_2$ (indeed $\phi_1(z) + bz = 0$ if and only if $z = 0$ or $z^{\frac{3}{4}} = b^{-1}$). Thus ϕ_1 satisfies condition (4.4). Note now that $\phi_3(z) = z\phi_1(\frac{1}{z})$. Therefore, according to assertion (5) of subsection 4.6.1 and since $\phi_1(0) = 0$, ϕ_3 satisfies condition (4.3) and (4.4). □

Therefore, collecting together Proposition 4.8.1, Proposition 4.8.2 and Lemma 4.8.3, we get

Proposition 4.8.4. *Let f be defined as*

$$\forall t \in \mathbb{F}_{2^n},\quad f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)\frac{1}{4}+1}) \tag{4.11}$$

with m odd, $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{2^n}^\star$. Then, f is bent if and only if $b^{2^m+1} = a$.

Remark 4.8.5. *Dobbertin et al. showed that if $b^{2^m+1} = a$ then function f is bent. We have shown here that the converse is true.*

Remark 4.8.6. *We can see that the function f belongs, up to affine equivalence, to the sub-class of $\mathcal{H}$ described in 4.6.1 (with $i = m - 2$). In particular, it belongs to the completed Maiorana-McFarland class (see e.g. [31])*

Let us now compute the dual function of f. Since we have, in parallel, bivariate and univariate representations for the same functions, we first need to clarify how the duals are related in such general context. Given a basis (u, v) of the 2-dimensional vector space $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$, let $g(x, y) = f(ux + vy)$, $x, y \in \mathbb{F}_{2^m}$. For every $w \in \mathbb{F}_{2^n}$ we have $\widehat{\chi_f}(w) = \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{g(x,y)+\mathrm{Tr}_1^n(w(ux+vy))} = \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{g(x,y)+\mathrm{Tr}_1^m(x\,\mathrm{Tr}_m^n(wu)+y\,\mathrm{Tr}_m^n(wv))}$. Hence the value of $\widehat{\chi_f}(w)$ is related in a natural way to the decomposition of w over a dual basis of (u, v), that is, a basis (u', v') such that $\mathrm{Tr}_m^n(uu') = \mathrm{Tr}_m^n(vv') = 1$ and $\mathrm{Tr}_m^n(uv') = \mathrm{Tr}_m^n(u'v) = 0$, the decomposition of w over this basis being then $w = \mathrm{Tr}_m^n(uw)u' + \mathrm{Tr}_m^n(vw)v'$. In such context we have $\widehat{\chi_f}(au' + bv') = \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{g(x,y)+\mathrm{Tr}_1^m(ax+by)} = \widehat{\chi_g}(a, b)$. Since there is no reason why g and its dual should be calculated with respect to different bases, we are then drawn to choose the basis (u, v) autodual.

Lemma 4.8.7. *Let (u,v) be an autodual basis of the 2-dimensional vector space $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$. Let f be any bent function over $\mathbb{F}_{2^n}$ and $g(x,y)=f(ux+vy)$, $x,y\in\mathbb{F}_{2^m}$, its bivariate expression with respect to the basis (u,v). Then we have $\widehat{\chi_f}(au+bv)=\widehat{\chi_g}(a,b)$ where $\widehat{\chi_f}$ is calculated with respect to the inner product $w\cdot t=\mathrm{Tr}_1^n(wt)$ in $\mathbb{F}_{2^n}$ and $\widehat{\chi_g}$ is calculated with respect to the inner product $(a,b)\cdot(x,y)=\mathrm{Tr}_1^m(ax+by)$ in $\mathbb{F}_{2^m}^2$.*

We need then to make a choice of an autodual basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$. This will be simplified if we assume that $b^4\neq a^2$. Then there exists $v\in\mathbb{F}_{2^n}$ such that $\mathrm{Tr}_m^n(v)=1$ and $b^4=a^2v^{2^m-1}$. Such an element v is unique. Then we can take $u=v^{2^m}$ (indeed, v and v^{2^m} are linearly independent: suppose that there exists $z\in\mathbb{F}_{2^m}^\star$ such that $v^{2^m}=zv$; then $v^{2^m-1}=z$, that is, $(v^{2^m-1})^{2^m-1}=v^{2(1-2^m)}=1$, a contradiction with $b^4=a^2v^{2^m-1}$ and $b^4\neq a^2$) and the basis (u,v) is then clearly autodual. We define then $g:\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}\to\mathbb{F}_{2^n}$ as: $\forall(x,y)\in(\mathbb{F}_{2^m})^2, g(x,y)=f(v^{2^m}x+vy)$, where $b^4=a^2v^{2^m-1}$. According to Proposition 4.6.3, the dual function $\widetilde{f}$ of f satisfies $\widetilde{f}(w)=1$ if and only if the equation $\psi(z)+\mathrm{Tr}_m^n(vw)z+\mathrm{Tr}_m^n(v^{2^m}w)=0$ has no solution in $\mathbb{F}_{2^m}$ where $\psi(z)=G(z)+\mu z$ is given by:

$$\psi^4(z)=a^2u^{2(2^m+1)}+\mathrm{Tr}_m^n(b^4u^{2^m+3})+\mathrm{Tr}_m^n(v^{2^m}u)\,\mathrm{Tr}_m^n(b^4u^2)z+(a^2v^{2(2^m+1)}+\mathrm{Tr}_m^n(b^4v^{2^m+3}))z^4.$$

Let us simplify a little the above expression by noting that, for $u=v^{2^m}$ and $b^4=a^2v^{2^m-1}$:

$$\begin{aligned}\mathrm{Tr}_m^n(b^4u^{2^m+3})&=a^2\,\mathrm{Tr}_m^n(v^{2^m-1+1+3\cdot2^m})=a^2\,\mathrm{Tr}_m^n(v^{2^{m+2}})=a^2\,\mathrm{Tr}_m^n(v)^{2^{m+2}}=a^2\\ \mathrm{Tr}_m^n(v^{2^m}u)&=\mathrm{Tr}_m^n(v^{2^{m+1}})=\mathrm{Tr}_m^n(v)^{2^{m+1}}=1\\ \mathrm{Tr}_m^n(b^4v^{2^m+3})&=a^2\,\mathrm{Tr}_m^n(v^{2(2^m+1)})=a^2v^{2(2^m+1)}\,\mathrm{Tr}_m^n(1)=0.\end{aligned}$$

Furthermore, note that $\mathrm{Tr}_m^n(v)=1=v+v^{2^m}$ and then that $v^{-1}=1+v^{2^m-1}$ that is, $v^{2^m-1}=1+v^{-1}$. Therefore,

$$\begin{aligned}\mathrm{Tr}_m^n(b^4u^2)&=a^2\,\mathrm{Tr}_m^n(v^{2^m-1}v^{2^{m+1}})=a^2\big(\mathrm{Tr}_m^n(v^{2^{m+1}})+\mathrm{Tr}_m^n(v^{2^m}v^{2^m-1})\big)\\&=a^2\big(1+\mathrm{Tr}_m^n(v^{2^m-1})+\mathrm{Tr}_m^n(v^{2^m})\big)=a^2\,\mathrm{Tr}_m^n(v^{2^m-1})\\&=a^2(\mathrm{Tr}_m^n(1+v^{-1}))=a^2\,\mathrm{Tr}_m^n(v^{-1}).\end{aligned}$$

We have also $\mu=a^{1/2}v^{(2^m+1)/2}+\mathrm{Tr}_m^n(bv^{(2^m-1)\frac14+1})=a^{1/2}(v^{(2^m+1)/2}+\mathrm{Tr}_m^n(v^{(2^m+1)/2}))=a^{1/2}v^{(2^m+1)/2}$ (since $v^{(2^m+1)/2}\in\mathbb{F}_{2^m}$ and therefore $\mathrm{Tr}_m^n(v^{(2^m+1)/2}))=0$).

We thus obtain that $\psi^4(z)=a^2(v^{2(2^m+1)}+1)+a^2\,\mathrm{Tr}_m^n(v^{-1})z+a^2v^{2(2^m+1)}z^4$, that is:

$$\psi^4(z)=a^2\big(v^{2(2^m+1)}+1+\mathrm{Tr}_m^n(v^{-1})z+v^{2(2^m+1)}z^4\big).$$

The support of the dual function of f is thus defined as:
$\widetilde{f}(a^{\frac12}w)=1$ if and only if the equation $v^{\frac{2^m+1}{2}}+1+\mathrm{Tr}_m^n(v^{2^m}w)+\mathrm{Tr}_m^n(v^{-\frac14})z^{\frac14}+(v^{\frac{2^m+1}{2}}+\mathrm{Tr}_m^n(vw))z=0$ has no solution in $\mathbb{F}_{2^m}$. Note that $\frac{2^m+1}{2}=(2^m-1)\frac12+1$.

Now, we have the following Lemma

Lemma 4.8.8. *([44]) Let σ, ρ, τ be three elements of $\mathbb{F}_{2^m}$. Assume that $\sigma\neq0$. Let $N=\#\{z\in\mathbb{F}_{2^m}\mid\ \sigma z+\rho z^{\frac14}=\tau\}$. Then, $N=\begin{cases}2 & \text{if } \mathrm{Tr}_1^m\left(()\,\frac{\tau}{\sigma}\cdot\frac{1}{\lambda}\right)=0 \text{ where } \lambda=(\frac{\rho^4}{\sigma^4})^{\frac13}\\ 0 & \text{otherwise.}\end{cases}$*

Proof. Rewrite the equation $\sigma z+\rho z^{\frac14}=\tau$ as $\lambda\big((\frac{z}{\lambda})+\frac{\rho}{\sigma}\frac{1}{\lambda^{\frac34}}(\frac{z}{\lambda})^{\frac14}\big)=\frac{\tau}{\sigma}$. Choose λ such that $\lambda^{\frac34}=\frac{\rho}{\sigma}$ (m being odd, the mapping $\lambda\mapsto\lambda^3$ is a permutation of $\mathbb{F}_{2^m}$ and therefore the mapping $\lambda\mapsto\lambda^{3/4}$ as well).

Then, $N = \#\{t \in \mathbb{F}_{2^m} \mid t + t^{\frac{1}{4}} = \frac{\tau}{\sigma} \cdot \frac{1}{\lambda}\}$.
The map $t \in \mathbb{F}_{2^m} \mapsto t + t^{\frac{1}{4}}$ is linear; its kernel is equal to $\mathbb{F}_2$ (since $t + t^{\frac{1}{4}} = 0 \iff t = 0$ or $t^{\frac{3}{4}} = 1 \iff t = 0$ or $t = 1$), hence its image E has dimension $m-1$ and equals then $\{\delta \in \mathbb{F}_{2^m} \mid \mathrm{Tr}_1^m(\delta) = 0\}$ (indeed, for every element $\delta = t + t^{\frac{1}{4}}$ of E, one has $\mathrm{Tr}_1^m(\delta) = \mathrm{Tr}_1^m(t) + \mathrm{Tr}_1^m(t)^{\frac{1}{4}} = 0$). This implies that N equals 2 if $\mathrm{Tr}_1^m(\frac{\tau}{\sigma} \cdot \frac{1}{\lambda}) = 0$ and is null otherwise, proving the result.

□

We deduce:

Theorem 4.8.9. *([44]) Let $n = 2m$ with m odd and f be defined as*

$$\forall t \in \mathbb{F}_{2^n}, \quad f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)\frac{1}{4}+1})$$

where $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{2^n}^\star$ are such that $b^{2^m+1} = a$ and $b^4 \neq a^2$. Let v be such that $\mathrm{Tr}_m^n(v) = 1$ and $b^4 = a^2 v^{2^m-1}$. Then the dual of f is such that

$$\widetilde{f}(a^{\frac{1}{2}}w) = \mathrm{Tr}_1^m\left(\left(v^{\frac{2^m+1}{2}} + 1 + \mathrm{Tr}_m^n(v^{2^m}w)\right)\left(\frac{\mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}}{\mathrm{Tr}_m^n(v^{-1})}\right)^{\frac{1}{3}}\right).$$

It has algebraic degree $\frac{m+3}{2}$. Hence, for $m > 3$, $\widetilde{f}$ is EA-inequivalent to the functions introduced in [93].

Proof. Applying Lemma 4.8.8 with $\sigma = \mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}$, $\rho = \mathrm{Tr}_m^n(v^{-\frac{1}{4}})$ and $\tau = v^{\frac{2^m+1}{2}} + 1 + \mathrm{Tr}_m^n(v^{2^m}w)$, we deduce that $\widetilde{f}(a^{\frac{1}{2}}w) = 1$ if and only if

$$\mathrm{Tr}_1^m\left(\frac{v^{\frac{2^m+1}{2}} + 1 + \mathrm{Tr}_m^n(v^{2^m}w)}{\mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}}\left(\frac{\mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}}{\mathrm{Tr}_m^n(v^{-1/4})}\right)^{\frac{4}{3}}\right) = 1$$

that is

$$\widetilde{f}(a^{\frac{1}{2}}w) = \mathrm{Tr}_1^m\left(\left(v^{\frac{2^m+1}{2}} + 1 + \mathrm{Tr}_m^n(v^{2^m}w)\right)\left(\frac{\mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}}{\mathrm{Tr}_m^n(v^{-1})}\right)^{\frac{1}{3}}\right).$$

For every element z of $\mathbb{F}_{2^m}$ we have $z^{1/3} = z^{1+4+4^2+4^3+\cdots+4^{\frac{m-1}{2}}}$. Hence, the vectorial function $\left(\frac{\mathrm{Tr}_m^n(vw)+v^{\frac{2^m+1}{2}}}{\mathrm{Tr}_m^n(v^{-1})}\right)^{\frac{1}{3}}$ has algebraic degree $\frac{m+1}{2}$. Since the functions $v^{\frac{2^m+1}{2}} + 1 + \mathrm{Tr}_m^n(v^{2^m}w)$ and $\mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}$ are affinely independent over $\mathbb{F}_{2^m}$, we deduce that the degree of the dual is $\frac{m+3}{2}$. Since the algebraic degree is affinely invariant, and since for $m > 3$, $\frac{m+3}{2}$ is different from 3 and m, this proves that $\widetilde{f}$ is inequivalent to the functions introduced in [93]. □

This gives an answer to the open question evoked in [93]: at least one of the duals of the functions introduced in this paper is affinely inequivalent to them.

Remark 4.8.10. *Function $\widetilde{f}$ in Theorem 4.8.9 is affinely equivalent to the bivariate function $g(x, y) = xy^{1/3}$. The function $y \in \mathbb{F}_{2^m} \mapsto y^{1/3} \in \mathbb{F}_{2^m}$ is a permutation and $\widetilde{f}$ belongs then to the completed Maiorana-McFarland class (but we knew this already thanks to Remark 4.8.6, since the dual of a function in the completed Maiorana-McFarland class belongs to this same class (see e.g. [31])).*

4.8.2 On the duals of the known bent functions with 2^r Niho exponents

We have seen in Subsection 4.4.2 that an extension of the second class of Niho bent from [93] has the form:

$$\mathrm{Tr}_1^n\left(at^{2^m+1}+\sum_{i=1}^{2^{r-1}-1}t^{(2^m-1)\frac{i}{2^r}+1}\right)$$

with $r>1$ satisfying $\gcd(r,m)=1$ and $a\in\mathbb{F}_{2^n}$ is such that $a+a^{2^m}=1$.

Recall that the class $\mathcal{H}$ introduced in the previous section is defined as the set of (bent) functions g satisfying

$$g(x,y)=\begin{cases}\mathrm{Tr}_1^m\left(xH\left(\frac{y}{x}\right)\right), & \text{if} \quad x\neq 0\\ \mathrm{Tr}_1^m(\mu y), & \text{if} \quad x=0\end{cases}, \tag{4.12}$$

where $\mu\in\mathbb{F}_{2^m}$ and H is a mapping from $\mathbb{F}_{2^m}$ to itself satisfying the following necessary and sufficient conditions

$$G: z\mapsto H(z)+\mu z \text{ is a permutation on } \mathbb{F}_{2^m} \tag{4.13}$$

$$z\mapsto G(z)+\beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta\in\mathbb{F}_{2^m}^*. \tag{4.14}$$

As proved in [44], condition (4.14) implies condition (4.13) and, thus, is necessary and sufficient for g being bent.

In the following proposition, we show that the bent function given above has the form of (4.12) and calculate the corresponding function G. By showing that G satisfies conditions (4.13) and (4.14), we give an alternative proof of the bentness.

Proposition 4.8.11. *([41],[14]) Let $r>1$ be a positive integer with $\gcd(r,m)=1$, $a\in\mathbb{F}_{2^n}$ with $a+a^{2^m}=1$ and Boolean function f over $\mathbb{F}_{2^n}$ be defined as*

$$f(t)=\mathrm{Tr}_1^n\left(at^{2^m+1}+\sum_{i=1}^{2^{r-1}-1}t^{(2^m-1)\frac{i}{2^r}+1}\right).$$

Take any $u\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$ and $v\in\mathbb{F}_{2^m}^*$. Then for any $x,y\in\mathbb{F}_{2^m}$,

$$f(ux+vy)=\begin{cases}\mathrm{Tr}_1^m(xH(y/x)), & \text{if} \quad x\neq 0\\ \mathrm{Tr}_1^m(vy), & \text{if} \quad x=0\end{cases}$$

and mapping G such that $G(z)=H(z)+vz$ can be expressed by

$$G^{2^r}(z)=(u+u^{2^m})^{2^r-1}vz+\frac{u^{2^m+2^r}+u^{2^{m+r}+1}}{u+u^{2^m}}$$

and satisfies conditions (4.13) and (4.14).

Proof. By the selection criteria, the pair (u,v) makes up a basis of $\mathbb{F}_{2^n}$ as a two-dimensional vector space over $\mathbb{F}_{2^m}$. Then every element $t\in\mathbb{F}_{2^n}$ can be uniquely written as $ux+vy$ with $(x,y)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$.

Now

$$\begin{aligned} f(ux+vy) &= \mathrm{Tr}_1^m\left(t^{2^m+1}\right) + \mathrm{Tr}_1^n\Big(\sum_{i=1}^{2^{r-1}-1} t^{(2^m-1)\frac{i}{2^r}+1}\Big) \\ &= \mathrm{Tr}_1^m\left((ux+vy)^{2^m+1}\right) \\ &\quad + \mathrm{Tr}_1^n\Big(\sum_{i=1}^{2^{r-1}-1} (ux+vy)^{(2^m-1)\frac{i}{2^r}+1}\Big) \end{aligned}$$

and for $x=0$, since $v \in \mathbb{F}_{2^m}^*$,

$$\begin{aligned} f(vy) &= \mathrm{Tr}_1^m\left((vy)^{2^m+1}\right) + \mathrm{Tr}_1^n\Big(\sum_{i=1}^{2^{r-1}-1} (vy)^{(2^m-1)\frac{i}{2^r}+1}\Big) \\ &= \mathrm{Tr}_1^m\left(vy\right) \ . \end{aligned}$$

For $x \neq 0$,

$$\begin{aligned} f(ux+vy) &= \mathrm{Tr}_1^m\Big((u+vy/x)^{2^m+1}x^2 \\ &\quad + \sum_{i=1}^{2^{r-1}-1} \mathrm{Tr}_m^n\Big((u+vy/x)^{(2^m-1)\frac{i}{2^r}+1}\Big)\, x\Big) \\ &= \mathrm{Tr}_1^m(xH(y/x)) \end{aligned}$$

with

$$\begin{aligned} H(z) &= (u+vz)^{(2^m+1)/2} \\ &\quad + \sum_{i=1}^{2^{r-1}-1} \mathrm{Tr}_m^n\Big((u+vz)^{(2^m-1)\frac{i}{2^r}+1}\Big) \end{aligned}$$

and $z \in \mathbb{F}_{2^m}$. Taking the latter identity to the power of 2^r we obtain

$$\begin{aligned} H^{2^r}(z) &= (u+vz)^{(2^m+1)2^{r-1}} \\ &\quad + \sum_{i=1}^{2^{r-1}-1} \mathrm{Tr}_m^n\Big((u+vz)^{(2^m-1)i+2^r}\Big) \\ &= (u+vz)^{(2^m+1)2^{r-1}} \\ &\quad + \mathrm{Tr}_m^n\big(\frac{(u+vz)^{(2^m+1)2^{r-1}} + (u+vz)^{2^m+2^r-1}}{(u+vz)^{2^m-1}+1}\big) \\ &= (u+vz)^{(2^m+1)2^{r-1}} \\ &\quad + \frac{(u+vz)^{(2^m+1)2^{r-1}} + (u+vz)^{2^m+2^r-1}}{(u+vz)^{2^m-1}+1} \\ &\quad + \frac{(u+vz)^{(2^m+1)2^{r-1}} + (u+vz)^{2^{m+r}-2^m+1}}{(u+vz)^{1-2^m}+1} \\ &= \frac{(u+vz)^{2^m+2^r} + (u+vz)^{2^{m+r}+1}}{(u+vz)^{2^m} + u + vz} \end{aligned}$$

$$= \frac{u^{2^m+2^r} + u^{2^m}(vz)^{2^r} + u^{2^r}vz}{u+u^{2^m}} + \frac{u^{2^{m+r}+1} + u^{2^{m+r}}vz + u(vz)^{2^r}}{u+u^{2^m}}$$

since $(u+vz)^{2^m-1} \neq 1$ (otherwise, $u^{2^m}+vz = u+vz$ meaning that $u \in \mathbb{F}_{2^m}$ that is a contradiction) and $u+vz \neq 0$. Therefore,

$$\begin{aligned} G^{2^r}(z) &= H^{2^r}(z) + (vz)^{2^r} \\ &= \frac{u^{2^m+2^r} + u^{2^r}vz + u^{2^{m+r}+1} + u^{2^{m+r}}vz}{u+u^{2^m}} \\ &= (u+u^{2^m})^{2^r-1}vz + \frac{u^{2^m+2^r} + u^{2^{m+r}+1}}{u+u^{2^m}} \ . \end{aligned}$$

Since $(u+u^{2^m})v \neq 0$, $G(z)$ is a permutation. Moreover, Condition (4.14) is equivalent to saying that for every $\rho \neq 0$, the linear function $L(z) = z + \rho z^{2^r}$ is 2-to-1 on $\mathbb{F}_{2^m}$. The latter holds since

$$L(z) = 0 \iff z = 0 \quad \text{or} \quad z = \rho^{1/(1-2^r)}$$

using that $\gcd(2^r-1, 2^m-1) = \gcd(r,m) = 1$. □

Note that taking $r = 2$, we immediately obtain the result of [44, Proposition 5] taking there $a = b = 1$. We can also conclude that function $f(t)$ belongs, up to affine equivalence, to the subclass of $\mathcal{H}$ built using Frobenius mappings $z \mapsto z^{2^{m-r}}$ with $\gcd(r,m) = 1$. As observed by Dillon, such bent functions belong to the completed class of $\mathcal{M}$ (see also [31]).

Also note that we can select u and v with $u + u^{2^m} = v = 1$. Then $u^{2^m} = u+1$ and

$$G^{2^r}(z) = z + u^{2^m+2^r} + u^{2^{m+r}+1} = z + u^{2^r} + u \ . \tag{4.15}$$

Choosing different basis results in equivalent polynomials $G(z)$. In the following lemma, we show how the Walsh transforms of a function in its univariate and bivariate representation, when choosing a specific basis, are related.

Lemma 4.8.12. *([41], [14]) Take any $u \in \mathbb{F}_{2^n}$ with $u + u^{2^m} = 1$. Then the pair $(u,1)$ makes up a basis of $\mathbb{F}_{2^n}$ as a two-dimensional vector space over $\mathbb{F}_{2^m}$ and for any $w \in \mathbb{F}_{2^n}$,*

$$\hat{\chi}_f(w) = \hat{\chi}_g\big(\operatorname{Tr}_m^n(uw), \operatorname{Tr}_m^n(w)\big) \ ,$$

where $g(x,y) = f(ux+y)$ for any $x, y \in \mathbb{F}_{2^m}$.

Proof. Any $w, t \in \mathbb{F}_{2^n}$ can be decomposed as $w = u\alpha + \beta$ and $t = ux + y$ with the uniquely defined $\alpha, \beta, x, y \in \mathbb{F}_{2^m}$. Then

$$\begin{aligned} \operatorname{Tr}_m^n(wt) &= \alpha x \operatorname{Tr}_m^n(u^2) + \alpha y \operatorname{Tr}_m^n(u) + \beta x \operatorname{Tr}_m^n(u) \\ &= (\alpha+\beta)x + \alpha y = \operatorname{Tr}_m^n(uw)x + \operatorname{Tr}_m^n(w)y \ . \end{aligned}$$

Therefore, the Walsh transform of a Boolean function f over $\mathbb{F}_{2^n}$ can be expressed in a point w as

$$\begin{aligned} \hat{\chi}_f(w) &= \sum_{t \in \mathbb{F}_{2^n}} (-1)^{f(t)+\operatorname{Tr}_1^n(wt)} \\ &= \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{g(x,y)+\operatorname{Tr}_1^m\left(\operatorname{Tr}_m^n(uw)x + \operatorname{Tr}_m^n(w)y\right)} \\ &= \hat{\chi}_g\big(\operatorname{Tr}_m^n(uw), \operatorname{Tr}_m^n(w)\big) \end{aligned}$$

as claimed. □

Now we can compute the univariate representation of the dual function of $f(t)$. Assuming conditions of Lemma 4.8.12 and using Proposition 4.6.3, the dual of $f(t)$ satisfies $\tilde{f}(w) = 1$ if and only if the equation $H(z) + \mathrm{Tr}_m^n(w)z + \mathrm{Tr}_m^n(uw) = 0$ has no solutions in $\mathbb{F}_{2^m}$. Using (4.15), the latter equation is equivalent to

$$(1 + w + w^{2^m})^{2^r} z^{2^r} + z + u^{2^r} + u + \left(uw + (uw)^{2^m}\right)^{2^r} = 0 \ .$$

If $1+w+w^{2^m} = 0$ then, obviously, the equation has a unique solution and $\tilde{f}(w) = 0$. Assuming $1 + w + w^{2^m} \neq 0$, with a substitution $z = (1 + w + w^{2^m})^{-2^r/(2^r-1)} s$ we obtain

$$s^{2^r} + s = \left(u^{2^r} + u + \left(uw + (uw)^{2^m}\right)^{2^r}\right)(1 + w + w^{2^m})^{2^r/(2^r-1)}$$

that has no solutions in $\mathbb{F}_{2^m}$ if and only if

$$\mathrm{Tr}_1^m \left(\left(u^{2^r} + u + \left(uw + (uw)^{2^m}\right)^{2^r}\right)(1 + w + w^{2^m})^{\frac{2^r}{2^r-1}}\right) = 1$$

since the linear mapping $s \mapsto s^{2^r} + s$ on $\mathbb{F}_{2^m}$ has the kernel of dimension one when $\gcd(r, m) = 1$. Using $u^{2^m} = u + 1$, the latter trace condition can be rewritten as

$$\mathrm{Tr}_1^m \left(\left(u(1 + w + w^{2^m}) + u^{2^{n-r}} + w^{2^m}\right) \times (1 + w + w^{2^m})^{1/(2^r-1)}\right) = 1 \ .$$

We deduce

Theorem 4.8.13. *([41], [14]) Let $n = 2m$, $r > 1$ be a positive integer with $\gcd(r, m) = 1$ and bent Boolean function f over $\mathbb{F}_{2^n}$ be defined as*

$$f(t) = \mathrm{Tr}_1^n \left(at^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} t^{(2^m-1)\frac{i}{2^r}+1}\right) \ ,$$

where $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. Take any $u \in \mathbb{F}_{2^n}$ with $u + u^{2^m} = 1$. Then the dual of $f(t)$ is equal to

$$\tilde{f}(w) = \mathrm{Tr}_1^m \left(\left(u(1 + w + w^{2^m}) + u^{2^{n-r}} + w^{2^m}\right) \times (1 + w + w^{2^m})^{1/(2^r-1)}\right) \ .$$

Moreover, if $d < m$ is a positive integer defined uniquely by $dr \equiv 1 \pmod m$ then the algebraic degree of $\tilde{f}(w)$ is equal to $d + 1$.

Proof. It remains to check the algebraic degree of $\tilde{f}(w)$. Since $\gcd(r, m) = 1$, positive integer d with the above prescribed properties exists and is defined uniquely. Then

$$\frac{1}{2^r - 1} \equiv \frac{2(2^{dr-1} - 1) + 1}{2^r - 1} = \frac{2^{dr} - 1}{2^r - 1} = 1 + 2^r + \cdots + 2^{(d-1)r} \pmod{2^m - 1}$$

is an integer having the binary weight d (also, if we reduce it modulo $2^m - 1$). Therefore, vectorial function $(1+w+w^{2^m})^{1/(2^r-1)}$ has algebraic degree d. Finally, functions $u(1+w+w^{2^m})+u^{2^{n-r}}+w^{2^m}$ and $(1 + w + w^{2^m})^{1/(2^r-1)}$ are affinely independent over $\mathbb{F}_{2^m}$ and this leads us to the claimed result. □

Note that $\tilde{f}(w)$ belongs to the completed class of $\mathcal{M}$ since this is a dual of a bent function $f(t)$ also belonging to this class (see, e.g., [31]). Moreover, $\tilde{f}(w)$ does not belong to class $\mathcal{H}$ since its restriction to any multiplicative coset of $\mathbb{F}_{2^m}$ (except when taking $\mathbb{F}_{2^m}$ itself) is not linear. In other words, $\tilde{f}(w)$ is not a Niho bent function. Also note that the dual of $f(t)$ does not depend on the chosen value of $u \in \mathbb{F}_{2^n}$ as long as $u + u^{2^m} = 1$. Indeed, all such values have the form of $u + c$ for every $c \in \mathbb{F}_{2^m}$. Inserting $u + c$ instead of u in the expression for $\tilde{f}(w)$ we obtain

$$\begin{aligned}
&\tilde{f}(w) + \mathrm{Tr}_1^m\left(\left(c(1+w+w^{2^m}) + c^{2^{n-r}}\right)(1+w+w^{2^m})^{1/(2^r-1)}\right)\\
&= \tilde{f}(w) + \mathrm{Tr}_1^m\left(c(1+w+w^{2^m})^{2^r/(2^r-1)} + c^{2^{n-r}}(1+w+w^{2^m})^{1/(2^r-1)}\right)\\
&= \tilde{f}(w) + \mathrm{Tr}_1^m\left(c^{2^{n-r}}(1+w+w^{2^m})^{1/(2^r-1)} + c^{2^{n-r}}(1+w+w^{2^m})^{1/(2^r-1)}\right)\\
&= \tilde{f}(w)\ .
\end{aligned}$$

4.9 Functions in class $\mathcal{H}$ and o-polynomials

Since the function studied above in Theorem 4.8.9 belongs to the completed Maiorana-McFarland class and since we do not know whether the other known Niho bent functions are in this same class, we are brought back to the question of knowing whether functions can be exhibited in class $\mathcal{H}$ which are not in the completed Maiorana-McFarland class. We observe now that Condition (4.4) implies Condition (4.3) and is equivalent to the fact that G is an *o-polynomial.*[7]

Definition 4.9.1. *Let m be any positive integer. A permutation polynomial G over $\mathbb{F}_{2^m}$ is called an o-polynomial (an oval polynomial) if, for every $\gamma \in \mathbb{F}_{2^m}$, the function*

$$z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$$

is a permutation of $\mathbb{F}_{2^m}$.

Note that some authors like Dobbertin in [91] add the condition "$G(0) = 0$, $G(1) = 1$" to the definition of o-polynomials; we do not include it since if it is not satisfied by an o-polynomial G, we can replace G by the o-polynomial $\frac{G(z)+G(0)}{G(1)+G(0)}$, which satisfies it.

Lemma 4.9.2. *([44]) Any function G from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ satisfies Condition* (4.4) *if and only if it is an o-polynomial.*

Proof. For every $\beta, \gamma \in \mathbb{F}_{2^m}$, the equation $G(z) + \beta z = G(\gamma) + \beta\gamma$ is satisfied by γ. Thus, if Condition (4.4) is satisfied, then for every $\beta \in {\mathbb{F}_{2^m}}^\star$ and every $\gamma \in \mathbb{F}_{2^m}$, there exists exactly one $z \in \mathbb{F}_{2^m}^\star$ such that $G(z+\gamma) + \beta(z+\gamma) = G(\gamma) + \beta\gamma$, that is, $\frac{G(z+\gamma)+G(\gamma)}{z} = \beta$. Then, for every $\gamma \in \mathbb{F}_{2^m}$, the function $z \in \mathbb{F}_{2^m}^\star \mapsto \frac{G(z+\gamma)+G(\gamma)}{z} \in \mathbb{F}_{2^m}^\star$ is bijective, that is, G and the function

[7] The notion of o-polynomial comes from Finite Projective Geometry. First of all, a projective space of dimension n over a finite field $\mathbb{F}_q$ is the set of any non-zero subspaces of ${\mathbb{F}_q}^{n+1}$ with respect to inclusion. This space is denoted by $PG_n(q)$. Let consider the case of projective space of dimension 2 (finite projective plane) over $\mathbb{F}_{2^n}$ i.e. $PG_2(2^n)$. A k-arc in $PG_2(2^n)$ is the set of k points no three collinear (i.e. there exists no line that contains any three points). The maximum cardinality of an arc in $PG_2(2^n)$ is $2^n + 2$. An *oval* of $PG_2(2^n)$ is an arc of cardinality $2^n + 1$ (i.e. a set of $2^n + 1$ points no three collinear). A *hyperoval* of $PG_2(2^n)$ is an arc of maximum cardinality (i.e. a set of $2^n + 2$ points no three collinear). Now certain type of polynomial give rise to hyperovals in $PG_2(2^n)$. More precisely, a polynomial f such that $D(f) = \{(1, t, f(t)), t \in \mathbb{F}_{2^n}\} \cup \{(0,1,0), (0,0,1)\}$ is a hyperoval is called an *o-polynomial.* A hyperoval of $PG_2(2^n)$ can then be represented by $D(f)$ where f is an o-polynomial. There is thus a close connection between "hyperovals" and "o-polynomials".

$z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$ are permutations. Hence, G is an o-polynomial. Conversely, if G is an o-polynomial, then for every $\gamma \in \mathbb{F}_{2^m}$, we have $\frac{G(z+\gamma)+G(\gamma)}{z} \neq 0$ for every $z \neq 0$ and for every $\beta \neq 0$ there exists exactly one nonzero z such that $G(z+\gamma)+G(\gamma) = \beta z$. Then for every $c \in \mathbb{F}_{2^m}$, either the equation $G(z) + \beta z = c$ has no solution, or it has at least a solution γ and then exactly one second solution $z + \gamma$ ($z \neq 0$). This completes the proof. □

A similar property was observed by Maschietti in [178] (as recalled by Dobbertin in [91]) for power functions. Maschietti was interested in cyclic difference sets while we are interested here in difference sets in elementary Abelian 2-groups (it is interesting to see that o-polynomials play a role in both frameworks). The fact that the result of Lemma 4.9.2 is true for general polynomials will have important consequences below.
Note that, according to the proof of Lemma 4.9.2, the property that for every $\gamma \in \mathbb{F}_{2^m}$, the function $z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$ is a permutation of $\mathbb{F}_{2^m}$ implies that G is a permutation of $\mathbb{F}_{2^m}$.
The simplest example of an o-polynomial is the already seen Frobenius automorphism $G(z) = z^{2^i}$ where i is coprime with n. Other known examples are the following:

1. $G(z) = z^6$ where m is odd [219];
2. $G(z) = z^{3 \cdot 2^k+4}$, where $m = 2k-1$ [111];
3. $G(z) = z^{2^k+2^{2k}}$, where $m = 4k-1$ [111];
4. $G(z) = z^{2^{2k+1}+2^{3k+1}}$, where $m = 4k+1$ [111];
5. $G(z) = z^{2^k} + z^{2^k+2} + z^{3 \cdot 2^k+4}$, where $m = 2k-1$ [133];
6. $G(z) = z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}}$ where m is odd [221]; note that $G(z) = D_5\left(z^{\frac{1}{6}}\right)$, where D_5 is the Dickson polynomial of index 5 [224];
7. $G(z) = \frac{\delta^2(z^4+z)+\delta^2(1+\delta+\delta^2)(z^3+z^2)}{z^4+\delta^2 z^2+1} + z^{1/2}$, where $\mathrm{Tr}_1^m(1/\delta) = 1$ and, if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$ [262];
8. $G(z) = \frac{1}{\mathrm{Tr}_m^n(v)}\left[\mathrm{Tr}_m^n(v^r)(z+1) + \mathrm{Tr}_m^n\left[(vz+v^{2^m})^r\right]\left(z + \mathrm{Tr}_m^n(v)z^{1/2}+1\right)^{1-r}\right] + z^{1/2}$, where m is even, $r = \pm\frac{2^m-1}{3}$, $v \in \mathbb{F}_{2^{2m}}$, $v^{2^m+1} = 1$ and $v \neq 1$ [263].

Remark 4.9.3. *To each o-polynomial G above correspond, according to Lemma 4.9.2 and to the observations made in 4.6.1, two Niho bent functions up to EA-equivalence: the one corresponding to G and the one corresponding to G^{-1}. We shall detail these bent functions below. Conversely, to every Niho bent function corresponds an o-polynomial. The question arises then of determining whether the o-polynomials we can deduce from the already known Niho bent functions are new up to o-equivalence (recall that the o-equivalence of polynomials has been defined in 4.6.1). We have seen above that the o-polynomial related to the Niho bent function of [93, Theorem 2] is a field automorphism (up to o-equivalence) and so is not new. The o-polynomial related to the function in [160] is also a Frobenius automorphism up to o-equivalence, as shown in the paper [41] (which extends the calculation of the dual to the generalization of the class given by Leander and Kholosha). The two other functions $f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)s+1})$ of [93, Theorems 1 and 3] (with $a = b^{2^m+1}$) lead to o-polynomials given by Relation (4.8). Different choices of the basis (u, v)*

give o-equivalent o-polynomials (since a change of basis is an $\mathbb{F}_{2^m}$-linear mapping). Different values of b give also o-equivalent o-polynomials because (as observed in [93]) the hypothesis on b allows writing that $b = \lambda^{(2^m-1)s+1}$ for some $\lambda \in \mathbb{F}_{2^n}$, and then $a = b^{2^m+1} = \lambda^{2^m+1}$ so that by multiplication of the variable t by $\frac{1}{\lambda}$ we can take $a = b = 1$ (the scalar multiplication is indeed an $\mathbb{F}_{2^m}$-linear mapping). For $s = 3$, taking $b = u = 1$ and $v \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, we get $G(z) = \left(1 + (v + v^{2^m})z\right)^{\frac{1}{2}} + \mathrm{Tr}_m^n\left((1 + vz)^{3\cdot 2^m-2} + (vz)^{3\cdot 2^m-2}\right)$. Choosing v in $U \setminus \{1\}$, that is, $v \neq 1$ such that $v^{2^m} = \frac{1}{v}$, then $\delta = v + v^{2^m}$ is any element of $\mathbb{F}_{2^m}$ such that $\mathrm{Tr}_1^m(1/\delta) = 1$ and we obtain $G(z) + 1 = (\delta z)^{\frac{1}{2}} + \frac{1+v^{-1}z+v^{-2}z^2+v^{-3}z^3}{1+v^2z^2} + \frac{1+vz+v^2z^2+v^3z^3}{1+v^{-2}z^2} + \left(v^{-5} + v^5\right)z = (\delta z)^{\frac{1}{2}} + \frac{(v^{-1}+v+v^{-5}+v^5)z+(v^{-7}+v^7+v^{-3}+v^3)z^3+(v^{-4}+v^4)z^4}{1+(v^{-2}+v^2)z^2+z^4} = (\delta z)^{\frac{1}{2}} + \frac{(\delta^5+\delta^3)z+(\delta^5+\delta^3+\delta)z^3+\delta^4z^4}{1+\delta^2z^2+z^4}$. We conjecture that this polynomial is o-equivalent to the o-polynomial numbered (7) above. For $s = \frac{1}{6}$ (m even), denoting $r = \frac{2^m-1}{3}$ and taking again $u = 1$ and v in $U \setminus \{1\}$, we get $G(z) = \left(1 + (v + v^{2^m})z\right)^{\frac{1}{2}} + \mathrm{Tr}_m^n\left((1 + vz)^{\frac{r}{2}+1} + (vz)^{\frac{r}{2}+1}\right) = \left(1 + (v + v^{2^m})z\right)^{\frac{1}{2}} + (1 + v^{\frac{1}{2}}z^{\frac{1}{2}})^r(1 + vz) + (1 + v^{\frac{-1}{2}}z^{\frac{1}{2}})^r(1 + v^{-1}z) + (vz)^{\frac{r}{2}+1} + (v^{-1}z)^{\frac{r}{2}+1}$. We conjecture that this polynomial is o-equivalent to the o-polynomial numbered (8) above.

For each of the six first o-polynomials G of the list above, we have two potentially new n-variable bent functions: $\mathrm{Tr}_1^m\left(xG\left(\frac{y}{x}\right)\right)$ and $\mathrm{Tr}_1^m\left(xG^{-1}\left(\frac{y}{x}\right)\right)$. For each of the two last ones, we have one potentially new bent function. We indicate now the bent functions we can obtain with the 6 first o-polynomials (we do not do the same for the two last o-polynomials since the situation with them needs to be clarified and since the expression of these bent functions would be complex - they are probably simpler in univariate form):

1. for m odd and $x, y \in \mathbb{F}_{2^m}$:

   - $f(x, y) = \mathrm{Tr}_1^m(x^{-5}y^6)$;
   - $f(x, y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$.

   The first function has algebraic degree $m - w_2(5) + w_2(6) = m$. Since in $\mathbb{Z}/(2^m - 1)\mathbb{Z}$ we have $\frac{1}{3} = \frac{2^{m+1}-1}{3} = 1 + 2^2 + 2^4 + \cdots + 2^{m-1}$ and therefore $w_2\left(\frac{1}{6}\right) = w_2\left(\frac{1}{3}\right) = \frac{m+1}{2}$ and $w_2\left(\frac{5}{6}\right) = w_2\left(\frac{5}{3}\right) = w_2\left(1 + \frac{2}{3}\right) = w_2\left(4 + 2^3 + 2^5 + \cdots + 2^{m-2}\right) = \frac{m-1}{2}$, the second function has degree m as well, which does not allow proving these two functions are EA-inequivalent; we leave open this question.

2. for $m = 2k - 1$ and $x, y \in \mathbb{F}_{2^m}$:

   - $f(x, y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$;
   - $f(x, y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$ (since the inverse of $3 \cdot 2^k + 4 \pmod{2^m - 1}$ equals $3 \cdot 2^{k-1} - 2$; indeed, $(3 \cdot 2^k + 4)(3 \cdot 2^{k-1} - 2) = 9 - 8 = 1 \pmod{2^m - 1}$).

   The first function has degree $m - w_2(3 \cdot (2^k + 1)) + w_2(3 \cdot 2^k + 4) = m - 4 + 3 = m - 1$ (if $k > 2$) and the second has degree $k + (k - 1) = 2k - 1 = m$ (if $k > 2$) since $-3 \cdot (2^{k-1} - 1) = 2^m - 3 \cdot 2^{k-1} + 2 = 2^{k-1}(2^k - 1 - 2) + 2 \pmod{2^m - 1}$ and $3 \cdot 2^{k-1} - 2 = 2^k + 2 \cdot (2^{k-2} - 1)$; hence the two functions are EA-inequivalent.

3. for $m = 4k - 1$ and $x, y \in \mathbb{F}_{2^m}$:

   - $f(x, y) = \mathrm{Tr}_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$;
   - $f(x, y) = \mathrm{Tr}_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$ (since the inverse of $2^k + 2^{2k} \pmod{2^m - 1}$ equals $1 - 2^{3k-1} + 2^{2k} - 2^k$; indeed, $(2^k + 2^{2k})(1 - 2^{3k-1} + 2^{2k} - 2^k) = 2^{m+1} - 1$).

The first function has degree $(3k-2)+2 = 3k$ since $2^m - 2^k - 2^{2k} = 2^k(2^{3k-1} - 1 - 2^k)$ and the second has degree $k + 2k = 3k$, which does not allow proving these two functions are EA-inequivalent; we leave open this question.

4. for $m = 4k+1$ and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^{2k+1}-2^{3k+1}} y^{2^{2k+1}+2^{3k+1}})$;
   - $f(x,y) = \mathrm{Tr}_1^m(x^{2^{3k+1}-2^{2k+1}+2^k} y^{1-2^{3k+1}+2^{2k+1}-2^k})$ (since the inverse of $2^{2k+1} + 2^{3k+1}$ [mod $2^m - 1$] equals $2^m - 2^{3k+1} + 2^{2k+1} - 2^k$).

   The first function has degree $(2k-1)+2 = 2k+1$ and the second has degree $(k+1)+(2k+1) = 3k+2$; hence the two functions are EA-inequivalent.

5. for $m = 2k-1$ and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^k} y^{2^k} + x^{-(2^k+1)} y^{2^k+2} + x^{-3\cdot(2^k+1)} y^{3\cdot 2^k+4})$;
   - $f(x,y) = \mathrm{Tr}_1^m\left(y\left(y^{2^k+1}x^{-(2^k+1)} + y^3x^{-3} + yx^{-1}\right)^{2^{k-1}-1}\right)$, since we have $G^{-1}(z) = z\left(z^{2^k+1} + z^3 + z\right)^{2^{k-1}-1}$ (see Lemma 4.9.4 below).

   The first function has degree $\max((k-1)+1, (2k-3)+2, (2k-5)+3) = 2k-1 = m$ (if $k > 2$). The second has also (optimal) algebraic degree m since its expansion contains the term $\mathrm{Tr}_1^m\left(y^{1+3\cdot(2^{k-1}-1)}x^{3\cdot(1-2^{k-1})}\right) = \mathrm{Tr}_1^m\left(y^{2^k+2^{k-1}-2}x^{2+(2^{2k-1}-2^{k-1})-2^k}\right)$. This does not allow proving these two functions are EA-inequivalent; we leave open this question.

6. for m odd and $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}} y^{\frac{1}{6}} + x^{\frac{1}{2}} y^{\frac{1}{2}} + x^{\frac{1}{6}} y^{\frac{5}{6}})$;
   - $f(x,y) = \mathrm{Tr}_1^m\left(x\left[D_{\frac{1}{5}}\left(\frac{y}{x}\right)\right]^6\right)$ where $D_{\frac{1}{5}}$ is the Dickson polynomial of index $\frac{1}{5}$, the inverse of 5 modulo $2^{2m}-1$ (see [224] or Remark 4.9.6 below); note that $\frac{1}{5} = 2^{2m} - 2^{2m-1} + 2^{2m-3} - 2^{2m-5} + ... + 2^7 - 2^5 + 2^3 - 2$ [mod $2^{2m}-1$].

   The first function has degree $\max(m, 2, m) = m$, since we already saw that $w_2\left(\frac{1}{6}\right) = \frac{m+1}{2}$ and $w_2\left(\frac{5}{6}\right) = \frac{m-1}{2}$. We leave open the question of an explicit expression of the second and of the determination of its algebraic degree.

Lemma 4.9.4. *([44])*
Let k be any positive integer and $m = 2k-1$. The inverse of function $z \in \mathbb{F}_{2^m} \mapsto z^{2^k} + 2^{2^k+2} + z^{3\cdot 2^k+4} \in \mathbb{F}_{2^m}$ equals: $z\left(z^{2^k+1} + z^3 + z\right)^{2^{k-1}-1}$.

Proof. Let $z' = z^{2^k}$ and $t \in \mathbb{F}_{2^m}$. The equation $z^{2^k} + 2^{2^k+2} + z^{3\cdot 2^k+4} = t$ is equivalent to $z' + z^2z' + z^4z'^3 = t$. Denoting $t' = t^{2^{k-1}}$, the 2^{k-1}-th power of this equation is $z + z'z + z'^2z^3 = t'$. Replacing z'^2z^3 by $z+z'z+t'$ in $t+z'+z^2z'+z^4z'^3 = 0$, we get $t+z'(1+zt')+z^2z'^2 = 0$. Multiplying by z and replacing again gives $t' + (t+1)z + t'z^2z' = 0$. For $t \neq 0$ (and therefore $z \neq 0$) we deduce $z' = \frac{t'+(t+1)z}{t'z^2}$ and replacing z' by this value in equation $t+z'(1+zt')+z^2z'^2 = 0$ allows eliminating z' and gives the equation $t + \frac{t'+(t+1)z}{t'z^2}(1+zt') + \frac{t'^2+(t^2+1)z^2}{t'^2z^2} = 0$; multiplying by t'^2z^2 gives $tt'^2z^2+(t'^2+(t+1)t'z)(1+zt')+t'^2+(t^2+1)z^2 = 0$ that is $(t+1+t'^2)t'z+(tt'^2+(t+1)t'^2+t^2+1)z^2 = 0$

and then we have $z = \frac{(t+1+t'^2)t'}{t'^2+t^2+1}$; hence $G^{-1}(z) = \frac{(z+1+z^{2^k})z^{2^{k-1}}}{z^{2^k}+z^2+1}$. Indeed, $z^{2^k}+z^2+1$ never vanishes (raising the equality $z^{2^k}+z^2+1=0$ to the 2^{k-1}-th power gives $z^{2^k}+z+1=0$ and implies $z^2+z=0$, and $z=0,1$ are not solutions of $z^{2^k}+z^2+1=0$) and the equality $G^{-1}(z) = \frac{(z+1+z^{2^k})z^{2^{k-1}}}{z^{2^k}+z^2+1}$ is true for $z=0$ as well. Since $(z^{2^k}+z^2+1)^{2^{k-1}} = z+1+z^{2^k}$, we deduce $G^{-1}(z) = \left(z^{2^k}+z^2+1\right)^{2^{k-1}-1} z^{2^{k-1}}$. □

Remark 4.9.5. *Another way for eliminating z' between the two equations $z^{2^k}+2^{2^k+2}+z^{3\cdot 2^k+4}=t$ and $z+z'z+z'^2z^3=t'$ is to use the resultant of the two polynomials in z' equal to $z'+z^2z'+z^4z'^3+t$ et $z+z'z+z'^2z^3+t'$ where z is considered as a parameter. But this leads to a more complex equation $z^3tt'+z^2t(t+1)t'+z(tt'+(t+1)^2(t'+1))+(t+1)t'^2=0$.*

Remark 4.9.6. *Let us recall why the inverse of D_α equals D_β with $\beta\alpha \equiv 1 \pmod{2^n-1}$ for every α co-prime with 2^n-1. Recall that $D_\alpha(D_\beta(y+\frac{1}{y})) = y^{\alpha\beta}+(\frac{1}{y})^{\alpha\beta}$ for every $y\in\mathbb{F}_{2^n}^\star$. Since every element $x\in\mathbb{F}_{2^m}^\star$ can be written as $x=c+\frac{1}{c}$ with $c\in\mathbb{F}_{2^n}$, we have $D_\alpha(D_\beta(x)) = D_\alpha(D_\beta(c+\frac{1}{c})) = c^{\alpha\beta}+(\frac{1}{c})^{\alpha\beta} = c+\frac{1}{c} = x$, proving that $D_\beta = D_\alpha^{-1}$ (note that $D_\alpha(0)=D_\beta(0)=0$).*

4.10 Niho Bent Functions and Subiaco/Adelaide hyperovals

The following section is from a joint work with Helleseth and Kholosha [126]. Recall that the first class of binomial bent function (via Niho exponent) of degree m given by Dobbertin at al. [93] has the following form:

$$f(t) = \mathrm{Tr}_1^n(\alpha_1 t^{d_1} + \alpha_2 t^{d_2})$$

where $2d_1 = 2^m+1 \in \mathbb{Z}/(2^n-1)\mathbb{Z}$ and $\alpha_1,\alpha_2 \in \mathbb{F}_{2^n}^*$ are such that $(\alpha_1+\alpha_1^{2^m})^2 = \alpha_2^{2^m+1}$. Equivalently, denoting $a=(\alpha_1+\alpha_1^{2^m})^2$ and $b=\alpha_2$ we have $a=b^{2^m+1}\in\mathbb{F}_{2^m}^*$ and

$$f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{d_2})$$

(note that if $b=0$ and $a\neq 0$ then f is also bent but becomes quadratic equals $\mathrm{Tr}_1^m(at^{2^m+1})$ with $a\in\mathbb{F}_{2^m}^*$) and $d_2=(2^m-1)3+1$ (with the condition that, if $m\equiv 2 \pmod 4$ then b is the fifth power of an element in $\mathbb{F}_{2^n}$; otherwise, b can be any nonzero element),

As was noted in [93], all cases except for $d_2=(2^m-1)3+1$ with $m\equiv 2 \pmod 4$ give $\gcd(d_2,2^n-1)=1$ and in the remaining case, $\gcd(d_2,2^n-1)=5$. Therefore, having the condition on b, it can be assumed, without loss of generality, that $b=1$ (this is achieved by substituting t with $b^{-1/d_2}t$). However, in Subsection 4.10.2, we show that even in the case when $m\equiv 2 \pmod 4$ the value of b can be taken arbitrary under the condition that $a=b^{2^m+1}$.

Since the restriction to $u\mathbb{F}_{2^m}$ of these bent functions is linear, they all belong to the class $\mathcal{H}$. The question left open in [93] was finding the dual and checking if that was of the Niho type (possibly up to affine equivalence). In this section, we find o-polynomials that arise from the first class of binomial Niho bent functions. However, it still remains to determine the dual. The third class is completely open.

4.10.1 Subiaco Hyperovals

Here we define o-polynomials that give rise to the Subiaco family of hyperovals.

Theorem 4.10.1 (Theorems 3-5 [65]). *Take polynomials $f(x)$ and $g(x)$ and for any $s \in \mathbb{F}_{2^m}$ define*

$$f_s(x) = \frac{f(x) + esg(x) + s^{1/2}x^{1/2}}{1 + es + s^{1/2}} \ , \tag{4.16}$$

where $e \in \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^m(e) = 1$ is defined further. Then in the following cases, $g(x)$ and $f_s(x)$ are o-polynomials:

(i) if m is odd then take $e = 1$ and

$$f(x) = \frac{x^2 + x}{(x^2 + x + 1)^2} + x^{\frac{1}{2}} \quad \text{and} \quad g(x) = \frac{x^4 + x^3}{(x^2 + x + 1)^2} + x^{\frac{1}{2}} \ ;$$

(ii) if $m \equiv 2 \pmod 4$ then take $e = w \in \mathbb{F}_{2^m}$ with $w^2 + w + 1 = 0$ and

$$f(x) = \frac{x^2(x^2 + wx + w)}{(x^2 + wx + 1)^2} + w^2x^{\frac{1}{2}} \quad \text{and} \quad g(x) = \frac{wx(x^2 + x + w^2)}{(x^2 + wx + 1)^2} + w^2x^{\frac{1}{2}} \ ;$$

(iii) for any m, take $e = \frac{w^2+w^5+w^{1/2}}{w(1+w+w^2)}$ where $w \in \mathbb{F}_{2^m}$ with $w^2 + w + 1 \neq 0$ and $\mathrm{Tr}_1^m(1/w) = 1$, and

$$f(x) = \frac{w^2(x^4 + x) + w^2(1 + w + w^2)(x^3 + x^2)}{(x^2 + wx + 1)^2} + x^{\frac{1}{2}} \quad \text{and}$$
$$g(x) = \frac{w^4x^4 + w^3(1 + w^2 + w^4)x^3 + w^3(1 + w^2)x}{(w^2 + w^5 + w^{1/2})(x^2 + wx + 1)^2} + \frac{w^{1/2}}{w^2 + w^5 + w^{1/2}}x^{\frac{1}{2}} \ .$$

It is useful to have the following explicit expressions for $f_s(x)$ in each of the cases considered. Denote $1 + es + s^{\frac{1}{2}} = A$, then $f_s(x)$ is equal to

$$\frac{s(x^4 + x^3) + x^2 + x}{A(x^2 + x + 1)^2} + x^{\frac{1}{2}} \ , \quad m \text{ odd} \tag{4.17}$$

$$A^{-1}\left(\frac{x^4 + w(sw + 1)(x^3 + x^2) + swx}{(x^2 + wx + 1)^2} + (w^2 + s + s^{\frac{1}{2}})x^{\frac{1}{2}}\right) \ , \quad m/2 \text{ odd} \tag{4.18}$$

$$\left(w^2\frac{(1 + sw + w^2)x^4 + (1 + w + w^2)^2(sx^3 + x^2) + (s + w + sw^2)x}{(1 + w + w^2)(x^2 + wx + 1)^2}\right. \tag{4.19}$$
$$\left. + \left(s^{\frac{1}{2}} + \frac{s + 1}{w^{1/2}(1 + w + w^2)}\right)x^{\frac{1}{2}}\right)(e + es + s^{\frac{1}{2}})^{-1} \ , \quad m \text{ arbitrary} \ ,$$

where in (4.19), we changed $s + 1$ for s in the original definition of $f_s(x)$. Note that for m odd, taking $w = 1$ in (4.19) results in (4.17).

In each of the cases listed above, the set $(f(x), g(x), a)$ defines a q-clan. On the other hand, by [65, Theorem 1], the existence of the q-clan is equivalent to the property that $g(x)$ is an o-polynomial and $f_s(x)$ is an o-polynomial for any $s \in \mathbb{F}_{2^m}$. In [222], it was shown that the Subiaco construction provides two inequivalent hyperovals if $m \equiv 2 \pmod 4$ and one hyperoval otherwise.

4.10.2 Bent Functions from Subiaco Hyperovals

First recall that in Section 4.6 we have extended the Class H of Dillon into a Class that we have denoted by $\mathcal{H}$. Such a class was defined as the set of (bent) functions g satisfying (4.12): $g(x,y) = \mathrm{Tr}_1^m\left(xH\left(\frac{y}{x}\right)\right)$ if $x \neq 0$ and $g(x,y)\,\mathrm{Tr}_1^m(\mu y)$ otherwise. where $\mu \in \mathbb{F}_{2^m}$ and H is a mapping from $\mathbb{F}_{2^m}$ to itself satisfying the following necessary and sufficient condition (4.13) (that is, $G : z \mapsto H(z) + \mu z$ is a permutation on $\mathbb{F}_{2^m}$ and condition (4.14) that is, $z \mapsto G(z) + \beta z$ is 2-to-1 on $\mathbb{F}_{2^m}$ for any $\beta \in \mathbb{F}_{2^m}^*$.

Moreover, recall that we have seen that condition (4.14) implies condition (4.13) and, thus, is necessary and sufficient for g being bent. It also follows that polynomials $G(z)$ satisfying (4.14) are so-called o-polynomials (oval polynomials) over $\mathbb{F}_{2^m}$ (the additional properties of $G(0) = 0$ and $G(1) = 1$ can be achieved by taking $\frac{G(z)+G(0)}{G(1)+G(0)}$ instead of $G(z)$). o-polynomials arise from hyperovals and define them. Note that class $\mathcal{H}$ contains all bent functions with the property that their restriction to the multiplicative cosets of $\mathbb{F}_{2^m}$ is linear.

Now, take the following function over $\mathbb{F}_{2^n}$

$$f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{3(2^m-1)+1}) \ ,$$

where $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_{2^n}^*$ are such that $b^{2^m+1} = a$. Let (u,v) be a basis of $\mathbb{F}_{2^n}$ as a two-dimensional vector space over $\mathbb{F}_{2^m}$. Then for any $x, y \in \mathbb{F}_{2^m}$, we obtain $f(ux+vy)$ having the form of (4.12) with

$$\begin{aligned} H(z) &= a^{\frac{1}{2}}(u+vz)^{\frac{2^m+1}{2}} + \mathrm{Tr}_m^n\left(b(u+vz)^{3(2^m-1)+1}\right) \\ \mu &= a^{\frac{1}{2}}v^{\frac{2^m+1}{2}} + \mathrm{Tr}_m^n(bv^{3(2^m-1)+1}) \ . \end{aligned}$$

Here we keep all the notation as above. Therefore, with $z \in \mathbb{F}_{2^m}$,

$$G(z) = a^{\frac{1}{2}}v^{\frac{2^m+1}{2}}z + a^{\frac{1}{2}}(u+vz)^{\frac{2^m+1}{2}} + \mathrm{Tr}_m^n\left(b(v^{3(2^m-1)+1}z + (u+vz)^{3(2^m-1)+1})\right) \ .$$

Further, we have that

$$(u+vz)^{\frac{2^m+1}{2}} = u^{\frac{2^m+1}{2}} + \left(\mathrm{Tr}_m^n(u^{2^m}v)\right)^{\frac{1}{2}}z^{\frac{1}{2}} + (vz)^{\frac{2^m+1}{2}}$$

and since $z \in \mathbb{F}_{2^m}$,

$$a^{\frac{1}{2}}v^{\frac{2^m+1}{2}}z + a^{\frac{1}{2}}(u+vz)^{\frac{2^m+1}{2}} = a^{\frac{1}{2}}u^{\frac{2^m+1}{2}} + a^{\frac{1}{2}}\left(\mathrm{Tr}_m^n(u^{2^m}v)\right)^{\frac{1}{2}}z^{\frac{1}{2}} \ . \tag{4.20}$$

Now expand the term $(u+vz)^{3(2^m-1)+1}$. To this end, note that $3(2^m-1)+1 = 2^{m+1}-1+2^m-1$. Then

$$\begin{aligned} (u+vz)^{3(2^m-1)+1} &= (u+vz)^{2^{m+1}-1}(u+vz)^{2^m-1} \\ &= \sum_{j=0}^{2^{m+1}-1} u^{2^{m+1}-1-j}(vz)^j \sum_{j=0}^{2^m-1} u^{2^m-1-j}(vz)^j \\ &= \sum_{i=0}^{3\cdot 2^m-2} (N_i \bmod 2)u^{3\cdot 2^m-2-i}(vz)^i \ , \end{aligned}$$

where $N_i = |E_i|$ and

$$E_i = \{(j_1,j_2) \mid j_1 + j_2 = i,\ 0 \le j_1 \le 2^{m+1}-1,\ 0 \le j_2 \le 2^m - 1\} \ .$$

We compute N_i by enumerating the elements of E_i as follows:

- for $0 \le i \le 2^m - 1$, we have $E_i = \{(i-j, j) \mid 0 \le j \le i\}$ and $N_i = i + 1$;
- for $2^m \le i \le 2^{m+1} - 1$, we have $E_i = \{(i-j, j) \mid 0 \le j \le 2^m - 1\}$ and $N_i = 2^m$;
- for $2^{m+1} \le i \le 3 \cdot 2^m - 2$, we have $E_i = \{(i-j, j) \mid i - 2^{m+1} + 1 \le j \le 2^m - 1\}$ and $N_i = 3 \cdot 2^m - 1 - i$ (indeed, $j_1 + j_2 = i$ implies that $j_2 = i - j_1 \ge i - 2^{m+1} + 1$ since $j_1 \le 2^{m+1} - 1$).

Therefore $N_i \bmod 2 = 1$ if and only if $i = 2l$ with $0 \le l \le 2^{m-1} - 1$ or $i = 2^{m+1} + 2l$ with $0 \le l \le 2^{m-1} - 1$ and

$$\begin{aligned}
(u+vz)^{3(2^m-1)+1} &= \sum_{l=0}^{2^{m-1}-1} u^{3\cdot 2^m-2-2l}(vz)^{2l} + \sum_{l=0}^{2^{m-1}-1} u^{3\cdot 2^m-2-2^{m+1}-2l}(vz)^{2^{m+1}+2l} \\
&\overset{(*)}{=} \sum_{l=0}^{2^{m-1}-1} u^{3\cdot 2^m-2(l+1)}(vz)^{2l} + \sum_{l=0}^{2^{m-1}-1} u^{2^m-2(l+1)}v^{2^{m+1}-2}(vz)^{2(l+1)} \\
&= \sum_{l=0}^{2^{m-1}-1} u^{3\cdot 2^m-2(l+1)}(vz)^{2l} + \sum_{l=1}^{2^{m-1}} u^{2^m-2l}v^{2^{m+1}-2}(vz)^{2l} \\
&= u^{3\cdot 2^m-2} + (u^{3\cdot 2^m-2} + u^{2^m}v^{2^{m+1}-2}) \sum_{l=1}^{2^{m-1}-1} \left(u^{-1}vz\right)^{2l} + v^{3\cdot 2^m-2}z \\
&= u^{3\cdot 2^m-2} + u^{2^m}(u^{2(2^m-1)} + v^{2(2^m-1)}) \left(1 + \frac{1 + (u^{-1}vz)^{2^m}}{1 + u^{-2}v^2z^2}\right) + v^{3\cdot 2^m-2}z \\
&= u^{2^m}v^{2(2^m-1)} + u^{2^m}(u^{2(2^m-1)} + v^{2(2^m-1)})(1 + u^{-1}vz)^{2^m-2} + v^{3\cdot 2^m-2}z \\
&= u^{2^m}v^{2(2^m-1)} + u^2(u^{2(2^m-1)} + v^{2(2^m-1)})(u+vz)^{2^m-2} + v^{3\cdot 2^m-2}z \ .
\end{aligned}$$

In the second sum after $(*)$, we used that $z^{2^{m+1}+2l} = (z^{2^m})^2 z^{2l} = z^2 z^{2l} = z^{2(l+1)}$. Finally, denoting

$$c = a^{\frac{1}{2}} u^{\frac{2^m+1}{2}} + \mathrm{Tr}_m^n(bu^{2^m}v^{2(2^m-1)})$$

and using (4.20), we obtain that

$$G(z) = c + a^{\frac{1}{2}} \left(\mathrm{Tr}_m^n(u^{2^m}v)\right)^{\frac{1}{2}} z^{\frac{1}{2}} + \mathrm{Tr}_m^n\left(bu^2(u^{2(2^m-1)} + v^{2(2^m-1)})(u+vz)^{2^m-2}\right) \ . \tag{4.21}$$

Now assume $v = 1$ and take $u \in \mathbb{F}_{2^n} \setminus \{1\}$ with $u^{2^m+1} = 1$ that means $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Also denote $u + u^{2^m} = w \in \mathbb{F}_{2^m}^*$ and observe that $\mathrm{Tr}_1^m(1/w) = 1$ (since this is equivalent to $u^2 + wu + 1$ being irreducible over $\mathbb{F}_{2^m}$). Moreover, all $w \in \mathbb{F}_{2^m}$ with such a trace property are obtained in this way from u. Then $u^{2^m-1} = w/u + 1$ and

$$\begin{aligned}
\mathrm{Tr}_m^n(u^{2^m}v) &= w \\
u^2\left(v^{2(2^m-1)} + u^{2(2^m-1)}\right) &= w^2 \ .
\end{aligned}$$

Under these conditions, $c = a^{\frac{1}{2}} + \mathrm{Tr}_m^n(bu^{2^m})$ and

$$\begin{aligned} G(z) &= c + (awz)^{\frac{1}{2}} + \frac{bw^2(u^{2^m}+z)}{(u+z)^2} + \frac{b^{2^m}w^2(u+z)}{(u^{2^m}+z)^2} \qquad (4.22)\\ &= c + (awz)^{\frac{1}{2}} + w^2\frac{b(u+w+z)^3 + b^{2^m}(u+z)^3}{(u+z)^2(u+w+z)^2}\\ &= c + (awz)^{\frac{1}{2}} + w^2\frac{(b+b^{2^m})(u+z)^3 + bw(z^2+wz+u^{2^m+1}+w^2)}{(z^2+wz+u^{2^m+1})^2}\\ &\overset{(4.23)}{=} c + (awz)^{\frac{1}{2}}\\ &\quad + \frac{w^2(b+b^{2^m})(z^3+uz^2+u^2z) + bw^3(z^2+wz) + \mathrm{Tr}_m^n(b^{2^m}(u^5+u))}{(z^2+wz+1)^2}\\ &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b^{2^m}u^5) + (awz)^{\frac{1}{2}}\\ &\quad + \frac{w^2(b+b^{2^m})(z^3+uz^2+u^2z) + bw^3(z^2+wz) + \mathrm{Tr}_m^n(b^{2^m}(u^5+u))(z^2+wz)^2}{(z^2+wz+1)^2}\\ &\overset{(4.24,4.25)}{=} a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b^{2^m}u^5) + (awz)^{\frac{1}{2}}\\ &\quad + \frac{\mathrm{Tr}_m^n(b^{2^m}(u^5+u))z^4 + \mathrm{Tr}_m^n(b)w^2z^3 + \mathrm{Tr}_m^n(b^{2^m}u^5)w^2z^2 + \mathrm{Tr}_m^n(b^{2^m}(u^4+1))z}{(z^2+wz+1)^2}\ . \end{aligned}$$

Here we used the following identities

$$w^2(b+b^{2^m})u^3 + bw^3(1+w^2) = \mathrm{Tr}_m^n(b^{2^m}(u^5+u))\ ; \qquad (4.23)$$

$$u(b+b^{2^m}) + bw + \mathrm{Tr}_m^n(b^{2^m}(u^5+u)) = \mathrm{Tr}_m^n(b^{2^m}u^5)\ ; \qquad (4.24)$$

$$w^2(b+b^{2^m})u^2 + bw^4 = \mathrm{Tr}_m^n(b^{2^m}(u^4+1))\ . \qquad (4.25)$$

Further, we consider three separate cases defined by the value of m.

The case m odd

In this case, take $u \in \mathbb{F}_4 \setminus \{0,1\}$. Note that $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and $w = u + u^{2^m} = u + u^2 = 1$. Then, by (4.22),

$$\begin{aligned} G(z) &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(bu) + (az)^{\frac{1}{2}} + \frac{\mathrm{Tr}_m^n(b)(z^4+z^3) + \mathrm{Tr}_m^n(bu)(z^2+z)}{(z^2+z+1)^2}\\ &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(bu) + (az)^{\frac{1}{2}} + a^{\frac{1}{2}}\frac{(B+B^{-1})(z^4+z^3) + (B^{-1}u^2+Bu)(z^2+z)}{(z^2+z+1)^2}\\ &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(bu) + a^{\frac{1}{2}}f_s(z)\ , \end{aligned}$$

where $B = ba^{-\frac{1}{2}}$ with $B^{-1} = b^{2^m}a^{-\frac{1}{2}} = B^{2^m}$ since $a = b^{2^m+1}$. Polynomial $f_s(z)$ with $s = \frac{1+B^2}{u^2+B^2u} \in \mathbb{F}_{2^m}$ is an o-polynomial (4.17) (assuming $u^2 + B^2u \neq 0$). In the case when $u^2 = B^2u$ (or, equivalently, $b^{2^m-1} = u^2$) we obtain

$$G(z) = bu + buz^{\frac{1}{2}} + bu\frac{z^4+z^3}{(z^2+z+1)^2} = bu(1+g(z))\ ,$$

since $a^{\frac{1}{2}} = (b^{2^m+1})^{\frac{1}{2}} = bu = b + b^{2^m}$ and where o-polynomial $g(z)$ comes from Theorem 4.10.1 Item (i).

Assuming $b^{2^m-1} \neq u^2$, note that equation $s = \frac{b^{2^m-1}+1}{b^{2^m-1}u^2+u}$ can be solved for the unknown $b \in \mathbb{F}_{2^n}^*$ for any $s \in \mathbb{F}_{2^m}$ since $s \neq u$. We conclude that the set of bent functions with $b \in \mathbb{F}_{2^n}^*$ corresponds exactly to all o-polynomials described in Theorem 4.10.1 Item (i). This means that the existence of this set of bent functions is equivalent to the existence of the corresponding q-clan.

The case $m \equiv 2 \pmod 4$

In this case, take $u \in \mathbb{F}_{16} \setminus \mathbb{F}_4$ with $u^5 = 1$. Note that $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and $u^{2^m+1} = u^5 = 1$. Then $u + u^{2^m} = u + u^4 = w \in \mathbb{F}_4 \subset \mathbb{F}_{2^m}$. Obviously, $w \neq 0$. It can be checked directly that u with the prescribed properties also satisfies $w \neq 1$ and, thus, $w^2 + w = 1$. There are *four* options for choosing u with these properties and both $w \in \mathbb{F}_4 \setminus \{0, 1\}$ can be obtained. Then, by (4.22),

$$\begin{aligned} G(z) &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + (awz)^{\frac{1}{2}} \\ &\quad + \frac{\mathrm{Tr}_m^n(b(u^4+1))z^4 + \mathrm{Tr}_m^n(b)w^2(z^3+z^2) + \mathrm{Tr}_m^n(b(u+1))z}{(z^2+wz+1)^2} \\ &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + (awz)^{\frac{1}{2}} + \mathrm{Tr}_m^n(b(u^4+1))\frac{z^4 + w(sw+1)(z^3+z^2) + swz}{(z^2+wz+1)^2} \\ &\overset{(*)}{=} a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + (1 + ws + s^{\frac{1}{2}})\,\mathrm{Tr}_m^n(b(u^4+1))f_s(z) \ , \end{aligned}$$

where polynomial $f_s(z)$ with $s = \frac{w^2\,\mathrm{Tr}_m^n(b(u+1))}{\mathrm{Tr}_m^n(b(u^4+1))}$ is an o-polynomial (4.18) (assuming $\mathrm{Tr}_m^n(b(u^4+1)) \neq 0$). In the case when $\mathrm{Tr}_m^n(b(u^4+1)) = 0$ (or, equivalently, $b^{2^m-1} = (u+1)^3 = u^4$) we obtain

$$\begin{aligned} G(z) &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + (awz)^{\frac{1}{2}} + \frac{\mathrm{Tr}_m^n(b)w^2(z^3+z^2) + \mathrm{Tr}_m^n(b(u+1))z}{(z^2+wz+1)^2} \\ &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + bu^2w^2z^{\frac{1}{2}} + bu^2\frac{wz(z^2+z+w^2)}{(z^2+wz+1)^2} \\ &= a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + bu^2 g(z) \ , \end{aligned}$$

since $a = b^{2^m+1} = b^2u^4$ and $\mathrm{Tr}_m^n(b)w = b(1+u^4)(u+u^4) = bu^2$ and where o-polynomial $g(z)$ comes from Theorem 4.10.1 Item (ii). On the other hand, if $b^{2^m-1} = u^4$ then it suffices just to take another u with the above defined properties (recall that four options exist). To obtain $(*)$ we used the following identities

$$\begin{aligned} &(w + s^2 + s)\,\mathrm{Tr}_m^n(b(u^4+1))^2 \\ &= w\,\mathrm{Tr}_m^n(b(u^4+1))^2 + w\,\mathrm{Tr}_m^n(b(u+1))^2 + w^2\,\mathrm{Tr}_m^n(b(u+1))\,\mathrm{Tr}_m^n(b(u^4+1)) \\ &= w^2\big(\mathrm{Tr}_m^n(bu)\,\mathrm{Tr}_m^n(bu^4) + \mathrm{Tr}_m^n(b)\,\mathrm{Tr}_m^n(b(u^4+u)) + \mathrm{Tr}_m^n(b)^2\big) + w\,\mathrm{Tr}_m^n(b(u^4+u))^2 \\ &= w^2(bu + b^{2^m}u^4)(bu^4 + b^{2^m}u) + w^2\,\mathrm{Tr}_m^n(b)^2 = aw \ . \end{aligned}$$

It is important to observe that there are no restrictions on the value of b here. It means that this technique allows to enlarge the original class of Niho bent functions proved in [93].

Assuming $b^{2^m-1} \neq u^4$, note that equation $s = \frac{w^2\,\mathrm{Tr}_m^n(b(u+1))}{\mathrm{Tr}_m^n(b(u^4+1))}$ can be solved for the unknown $b \in \mathbb{F}_{2^n}^*$ for any $s \in \mathbb{F}_{2^m}$. Indeed, this equation can be rewritten as

$$\begin{aligned} b(u^4s + s + uw^2 + w^2) &= b^{2^m}(us + s + u^4w^2 + w^2) \quad \text{or} \\ b(u^4s + s + u^4 + u^2) &= b^{2^m}(us + s + u^3 + u) \ . \end{aligned}$$

Since $s \in \mathbb{F}_{2^m}$, it is easy to see that this equation has nonzero sides and its right-hand side is a 2^mth power of the left-hand side. We conclude that the set of bent functions with $b \in \mathbb{F}_{2^n}^*$ corresponds exactly to all o-polynomials described in Theorem 4.10.1 Item (ii). This means that the existence of this set of bent functions is equivalent to the existence of the corresponding q-clan.

The case $m \equiv 0 \pmod 4$

In this case, $w^2+w+1 \neq 0$ since the opposite is equivalent to $u^4+u^3+u^2+u+1=0$ that gives $u \in \mathbb{F}_{2^4}$ which is a contradiction because $\mathbb{F}_{2^4} \subset \mathbb{F}_{2^m}$. As was noted in Subsection **??**, without loss of generality, we can assume $b=a=1$. Then, by (4.22),

$$\begin{aligned} G(z) &= 1+\mathrm{Tr}_m^n(u^5)+(wz)^{\frac{1}{2}}+\frac{\mathrm{Tr}_m^n(u^5+u)z^4+\mathrm{Tr}_m^n(u^5)w^2z^2+\mathrm{Tr}_m^n(u^4)z}{(z^2+wz+1)^2} \\ &\overset{(*)}{=} 1+\mathrm{Tr}_m^n(u^5)+(wz)^{\frac{1}{2}}+\frac{(w^5+w^3)z^4+w^3(1+w+w^2)^2z^2+w^4z}{(z^2+wz+1)^2} \\ &= 1+\mathrm{Tr}_m^n(u^5)+(w^2+w^5+w^{\frac{1}{2}})f_0(z) \ , \end{aligned}$$

where $(*)$ follows by $w(1+w+w^2)^2=\mathrm{Tr}_m^n(u^5)$ and $f_0(z)$ is an o-polynomial from (4.19).

Remark 4.10.2. *In 2004, using computer calculations, the following sporadic bent function of Niho type was found by Kholosha. For $m=4$,*

$$f(t)=\mathrm{Tr}_1^m(t^{2^m+1})+\mathrm{Tr}_1^n\left(t^{5(2^m-1)+1}+t^{7(2^m-1)+1}\right) \ . \tag{4.26}$$

The question open since then is whether this function is a new one or if it is EA-equivalent to one of the known Niho bent functions. Here we resolve this open problem.

Take basis elements $v=1$ and u with $u+u^{2^m}=1$. Since

$$x^{16}+x+1=(1+x+x^3+x^4+x^5+x^6+x^8)(1+x^3+x^5+x^6+x^8) \ ,$$

we get that either

$$1+u+u^3+u^4+u^5+u^6+u^8=0 \quad or \quad 1+u^3+u^5+u^6+u^8=0 \ . \tag{4.27}$$

By direct calculations, we obtain that $\mu=1$ and

$$\begin{aligned} G_1(z) &= z+(u+z)^{\frac{2^m+1}{2}}+\mathrm{Tr}_m^n\left((u+z)^{76}+(u+z)^{106}\right) \\ &= 1+u+u^4+u^6+u^8+u^{10}+u^{12} \\ &\quad +(u^4+u^8)z^2+(1+u^2+u^8)z^4+z^6+(1+u^2+u^4)z^8+z^{10}+z^{12} \ , \end{aligned}$$

since $z^2+(u+z)^{2^m+1}=u^{2^m+1}+\mathrm{Tr}_m^n(u)z=u^{2^m+1}+z$. As observed in [44, Sec. 3.1.2], adding a constant to $G_1(z)$ results into EA-equivalent bent functions, thus, the constant term in $G_1(z)$ can be ignored. Define $\beta=1+u+u^4\in\mathbb{F}_{2^m}$ and note that $\beta^4=\beta+1$ and β is primitive in $\mathbb{F}_{2^m}$ (this is checked easily). Then, depending on (4.27), $G_1(z)$ without a constant term is respectively equal to either

$$\begin{aligned} &\beta^9z^2+\beta^2z^4+z^6+\beta^{11}z^8+z^{10}+z^{12} \quad or \\ &\beta^7z^2+\beta^2z^4+z^6+\beta^{12}z^8+z^{10}+z^{12} \ . \end{aligned}$$

Both polynomials belong to the list of 2040 *o-polynomials representing the Lunelli-Sce hyperoval (numbers* 119 *and* 120 *in the list [214]). By [11, Theorem 26], the Lunelli-Sce hyperoval is a member of the Subiaco family of hyperovals. Thus, it is natural to expect that function (4.26) is EA-equivalent to the following Niho bent function from Subsection 4.4.2*

$$f(t) = \mathrm{Tr}_1^m(t^{2^m+1}) + \mathrm{Tr}_1^n(t^{3(2^m-1)+1}) \tag{4.28}$$

with $m = 4$. *However, this does not come automatically since equivalent hyperovals do not necessarily correspond to EA-equivalent bent functions (see [44, Sec. 3.1.2]).*

Now, take basis elements $v = 1$ *and* $w = u^2$ *(where* u *is the second element in the basis chosen for analyzing function (4.26)) and recall that different choices of basis lead to EA-equivalent functions. Then* $w + w^{2^m} = 1$ *and using (4.21), we obtain that function (4.28) corresponds to the following polynomial*

$$\begin{aligned} G_2(z) &= w^{8(2^m+1)} + 1 + z^8 + \mathrm{Tr}_m^n\left((w+z)^{14}\right) \\ &= 1 + w + w^2 + w^4 + w^6 + w^{10} + w^{12} \\ &\quad + (1 + w^4 + w^8)z^2 + (1 + w^2 + w^8)z^4 + z^6 + (w^2 + w^4)z^8 + z^{10} + z^{12} \\ &= 1 + u + u^5 + u^9 + u^{12} \\ &\quad + (u + u^8)z^2 + (u + u^4)z^4 + z^6 + (u^4 + u^8)z^8 + z^{10} + z^{12} \ . \end{aligned}$$

Similarly, if $\eta = 1 + w + w^4 = \beta^2 \in \mathbb{F}_{2^m}$ *(obviously,* η *is also primitive in* $\mathbb{F}_{2^m}$ *and* $\eta^4 = \eta + 1$*) then, depending on (4.27) (where* u *is replaced by* w*),* $G_2(z)$ *without a constant term is respectively equal to either*

$$\begin{aligned} &\eta^7 z^2 + \eta^2 z^4 + z^6 + \eta^{12} z^8 + z^{10} + z^{12} \quad \textit{or} \\ &\eta^9 z^2 + \eta^2 z^4 + z^6 + \eta^{11} z^8 + z^{10} + z^{12} \end{aligned}$$

using the fact that the sum of all coefficients in the latter polynomials has to be equal to one. These are the same Lunelli-Sce o-polynomials as obtained before but in the reverse order.

Now observe that

$$G_2(z + u^4 + u^8) = c_u + (u^4 + u^8)z^2 + (1 + u^2 + u^8)z^4 + z^6 + (1 + u^2 + u^4)z^8 + z^{10} + z^{12},$$

where c_u *is a constant depending on* u. *Finally, note that the latter polynomial without the constant term* c_u *is exactly* $G_1(u)$ *without the constant term. Since adding a constant term to the argument of an o-polynomial is one of the transformations that preserves EA-equivalence of the corresponding bent functions (see [44, Sec. 3.1.2]), we conclude that bent functions (4.26) and (4.28) are EA-equivalent.*

4.10.3 Bent Functions from Adelaide Hyperovals

Here we define o-polynomials that give rise to the Adelaide family of hyperovals.

Theorem 4.10.3 (Theorem 3.1 [265])**.** *Assume* m *is even,* $n = 2m$ *and denote* $l = \frac{2^m-1}{3}$. *Take any* $\beta \in \mathbb{F}_{2^n} \setminus \{1\}$ *with* $\beta^{2^m+1} = 1$ *and define the following functions over* $\mathbb{F}_{2^m}$

$$\begin{aligned} f(x) &= \frac{\mathrm{Tr}_m^n(\beta^l)(x+1)}{\mathrm{Tr}_m^n(\beta)} + \frac{\mathrm{Tr}_m^n\left((\beta x + \beta^{-1})^l\right)}{\mathrm{Tr}_m^n(\beta)(x + \mathrm{Tr}_m^n(\beta)x^{1/2} + 1)^{l-1}} + x^{\frac{1}{2}} \quad \textit{and} \\ eg(x) &= \frac{\mathrm{Tr}_m^n(\beta^l)}{\mathrm{Tr}_m^n(\beta)}x + \frac{\mathrm{Tr}_m^n\left((\beta^2 x + 1)^l\right)}{\mathrm{Tr}_m^n(\beta)\,\mathrm{Tr}_m^n(\beta^l)(x + \mathrm{Tr}_m^n(\beta)x^{1/2} + 1)^{l-1}} + \frac{1}{\mathrm{Tr}_m^n(\beta^l)}x^{\frac{1}{2}} \ , \end{aligned}$$

where $e = \frac{\mathrm{Tr}_m^n(\beta^l)}{\mathrm{Tr}_m^n(\beta)} + \frac{1}{\mathrm{Tr}_m^n(\beta^l)} + 1$. *Then* $g(x)$ *and* $f_s(x)$ *(defined in (4.16)) are o-polynomials for any* $s \in \mathbb{F}_{2^m}$.

In particular, using that $\beta^{2^m} = \beta^{-1}$ we obtain that

$$e\,\mathrm{Tr}_m^n(\beta)\,\mathrm{Tr}_m^n(\beta^l) f_1(x) = \mathrm{Tr}_m^n(\beta^{2l}) + \frac{\mathrm{Tr}_m^n\left((x+\beta^2)^l\right)}{(x + \mathrm{Tr}_m^n(\beta)x^{1/2} + 1)^{l-1}} + \mathrm{Tr}_m^n(\beta)x^{\frac{1}{2}} \ .$$

For even m, take the following Niho bent function over $\mathbb{F}_{2^n}$

$$f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)\frac{1}{6}+1}) \ ,$$

where $\frac{1}{6} = \frac{2^{m-1}+1}{3}$ is an inverse of 6 modulo 2^m+1, $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_{2^n}^*$ are such that $b^{2^m+1} = a$. As noted above, without loss of generality, it can be assumed that $a = b = 1$.

Assume $v = 1$ and take $u \in \mathbb{F}_{2^n} \setminus \{1\}$ with $u^{2^m+1} = 1$ that means $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Then $(u, 1)$ is a basis of $\mathbb{F}_{2^n}$ as a two-dimensional vector space over $\mathbb{F}_{2^m}$. Then for any $x, y \in \mathbb{F}_{2^m}$, we obtain $f(ux + vy)$ having the form of (4.6.1) with

$$\begin{aligned} H(z) &= (z+u)^{\frac{2^m+1}{2}} + \mathrm{Tr}_m^n\left((z+u)^{(2^m-1)\frac{1}{6}+1}\right) \\ \mu &= 1 \ . \end{aligned}$$

Denote $d = (2^m-1)\frac{1}{6} + 1 = (2^{m-1}+1)l + 1$, where $l = \frac{2^m-1}{3}$. Then

$$2^{m+1}d \pmod{2^n-1} = (2^{m+1}+1)l + 2^{m+1} = (2^m+1)(2l+1) + 2l$$

and

$$\begin{aligned} \mathrm{Tr}_m^n\left((z+u)^{2d}\right) &= \mathrm{Tr}_m^n\left((z+u)^{2^{m+1}d}\right) \\ &= (z+u)^{(2^m+1)(2l+1)}\,\mathrm{Tr}_m^n\left((z+u)^{2l}\right) \\ &= (z^2 + \mathrm{Tr}_m^n(u)z + 1)^{2l+1}\,\mathrm{Tr}_m^n\left((z+u)^{2l}\right) \\ &= \frac{\mathrm{Tr}_m^n\left((z+u)^{2l}\right)}{(z^2 + \mathrm{Tr}_m^n(u)z + 1)^{l-1}} \end{aligned}$$

since $3l = 2^m - 1$ and $z^2 + \mathrm{Tr}_m^n(u)z + 1 \in \mathbb{F}_{2^m}$.

Therefore, with $z \in \mathbb{F}_{2^m}$ and assuming $u = \beta^2$,

$$\begin{aligned} G(z) &= 1 + \mathrm{Tr}_m^n(\beta)z^{\frac{1}{2}} + \frac{\mathrm{Tr}_m^n\left((z+\beta^2)^l\right)}{(z + \mathrm{Tr}_m^n(\beta)z^{1/2} + 1)^{l-1}} \\ &= 1 + \mathrm{Tr}_m^n(\beta^{2l}) + e\,\mathrm{Tr}_m^n(\beta)\,\mathrm{Tr}_m^n(\beta^l) f_1(z) \ . \end{aligned}$$

Note that currently the associate o-polynomials of all the known Niho bent functions have been identified.

Chapter 5

Hyper-bent functions

Contents

5.1 Definitions and properties

In [272], A. Youssef and G. Gong study the Boolean functions f on the field $\mathbb{F}_{2^n}$ (n even) such that $f(x^k)$ is bent for every k co-prime with $2^n - 1$. These functions are called *hyper-bent functions*. Obviously, hyper-bent functions are in particular bent. Therefore they exist only when n is even and, that their Hamming weight is even. Consequently, their polynomial form is

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}(a_j x^j) \tag{5.1}$$

where Γ_n, $o(j)$ are defined as above and $a_j \in \mathbb{F}_{2^{o(j)}}$.

The condition of hyper-bentness seems difficult to satisfy. However, A. Youssef and G. Gong show in [272] that hyper-bent functions exist. Their result is equivalent to the following (the definition of elements of the class $\mathcal{PS}_{ap}^{\#}$ is defined in included in Proposition 5.4.1)

Proposition 5.1.1. *([36]) All the functions of class $\mathcal{PS}_{ap}^{\#}$ are hyper-bent.*

5.2 Hyper-bent Boolean functions in symmetric cryptography

Hyper-bent functions are both of theoretical and practical interest. In fact, they were initially proposed by Golomb and Gong [116] as a component of S-boxes to ensure the security of symmetric cryptosystems. These functions are currently used in the Data Encryption Standard (DES). The idea behind the hyper-bent functions is to maximize the minimum distance to all Boolean functions coming from bijective monomials on $\mathbb{F}_{2^n}$ (that is, bijective functions whose expression is the absolute trace of a single power function), not just the affine monomial functions (that is, functions of the form $\mathrm{Tr}_1^n(ax)+\epsilon$; $a \in \mathbb{F}_{2^n}$, $\epsilon \in \mathbb{F}_2$). The first definition of hyper-bent functions was based on a property of the *extended Walsh–Hadamard transform* of Boolean functions (introduced by Golomb and Gong [116]).

Definition 5.2.1.

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega, k) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\omega \cdot x^k)}, \textit{ with } \gcd(k, 2^n - 1) = 1.$$

where "$\cdot$" is an inner product in $\mathbb{F}_{2^n}$

We have the following characterization of the hyper-bent functions in terms of the extended Walsh transform:

Proposition 5.2.2. *f is hyper-bent on $\mathbb{F}_{2^n}$ if and only if its extended Hadamard transform takes only the values $\pm 2^{\frac{n}{2}}$.*

Carlet and Gaborit [36] have proved that the algebraic degree of any hyper-bent function defined onr $\mathbb{F}_{2^n}$ is exactly $\frac{n}{2}$.

5.3 Hyper-bent Boolean functions in coding theory

5.3.1 Background on binary cyclic codes

In all this subsection, we refer to [98] and [68]. Let N be a positive integer relatively prime to 2. Let t be the order of 2 modulo N that is, the smallest positive integer a such that $2^a \equiv 1 \pmod{N}$. Let α be a primitive Nth root of unity in $\mathbb{F}_{2^t}$. Let $\mathcal{C}$ be a binary cyclic code of length N with generator polynomial $g(X)$ in the ring $R_N := \mathbb{F}_2[X]/(X^N - 1)$, consisting of the residue classes of $\mathbb{F}_2[X]$ modulo $X^N - 1$. The polynomial $g(X)$ is the unique monic polynomial of minimum degree in $\mathcal{C}$ and $g(X) = \prod_s \prod_{i \in C_s} (X - \alpha^i)$, where s runs through some subset of the 2-cyclotomic cosets C_s modulo N. Let $T = \bigcup_s C_s$ be the union of these 2-cyclotomic cosets. The roots of the unity $Z = \{\alpha^i \mid i \in T\}$ are called the zeroes of the code $\mathcal{C}$ and $\{\alpha^i \mid i \notin T\}$ are the non-zeroes of $\mathcal{C}$. The set T is called the defining set of $\mathcal{C}$. Every vector $f = (f_0, f_1, \cdots, f_{N-1})$, identified with the polynomial $f(X) = f_0 \oplus +f_1 X \oplus + \cdots \oplus f_{N-1}X^{N-1}$ belongs to $\mathcal{C}$ if and only if $f(\alpha^i) = 0$ for each $i \in T$. The defining set T of $\mathcal{C}$, and hence either the set of zeroes or the set of non-zeroes, completely determines $g(X)$. The dimension of $\mathcal{C}$ is $N - deg(g(X)) = N - \#T$. Now, if we consider binary cyclic codes in the primitive case, more precisely, we assume that $N = 2^n - 1$ for n a positive integer, the order of 2 modulo N equals n. If α is a primitive element of $\mathbb{F}_{2^n}$. then, the vector $f = (f_0, f_1, \cdots, f_{N-1})$ can be identified with the restriction of a Boolean function f to the set $\mathbb{F}_{2^n}^\star$, defined by $f(\alpha^i) = f_i$, for every integer $i \in \{0, \cdots, 2^n - 2\}$.
Given a cyclic code $\mathcal{C}$ of length N and dimension k, we can define the extended cyclic code $\hat{\mathcal{C}}$ of $\mathcal{C}$ as the set of vectors $(f_0 \oplus \cdots \oplus f_{N-1}, f_0, \cdots, f_{N-1})$. The obtained code $\hat{\mathcal{C}}$ is a linear code of

length $N+1$ and dimension k. The vector $(f_0 \oplus \cdots \oplus f_{N-1}, f_0, \cdots, f_{N-1})$ can be identified with a Boolean function f on $\mathbb{F}_{2^n}$ whose algebraic degree is smaller than n.

5.3.2 Extended cyclic codes and hyper-bent functions

There exists a relationship between cyclic codes and hyper-bent functions (see [36]). Recall that by definition, a Boolean function on $\mathbb{F}_{2^n}$ is hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime with $2^n - 1$. This implies that every hyper-bent function belongs to the intersection of all the images of the Reed-Muller codes of order $\frac{n}{2}$ by the mappings $f \mapsto f(x^i)$, where i is co-prime with $2^n - 1$. Consequently, all the hyper-bent functions on $\mathbb{F}_{2^n}$ belong to the extended cyclic code H_n whose zeroes are all the elements of the form α^{ij}, where i is co-prime with $2^n - 1$ and $1 \leq j \leq 2^n - 2$ with $1 \leq w_2(j) \leq \frac{n}{2} - 1$. The non-zeroes of H_n are the α^j's such that j is zero or j satisfies $w_2(ij) = \frac{n}{2}$ for any i co-prime with $2^n - 1$. Carlet and Gaborit deduce that all hyper-bent functions on $\mathbb{F}_{2^n}$ have algebraic degree $\frac{n}{2}$. Hence hyper-bent functions belong to $\mathcal{RM}(\frac{n}{2}, n) \setminus \mathcal{RM}(\frac{n}{2} - 1, n)$ (while bent functions belong to the Reed-Muller codes $\mathcal{RM}(\frac{n}{2}, n)$ of order $\frac{n}{2}$).
It has been proved in [36], that functions of the $\mathcal{PS}_{ap}$ (these functions are in fact hyper-bent see *e.g.* [36]) are some codewords of weight $2^{n-1} - 2^{\frac{n}{2}-1}$ of a subcode of H_n. The authors deduce that for some n, depending on the factorization of $2^n - 1$, the only hyper-bent functions on n variables are the elements of the class $\mathcal{PS}^{\#}_{ap}$ (see Proposition 5.4.1). Now, let A_n be the extended cyclic code whose non-zeroes are the power of α whose exponents are all the multiples of $2^{\frac{n}{2}} - 1$. Let B_n be the cyclic code with non-zeroes α^i for i element of the ring of integer modulo $2^n - 1$ which is symmetric (i is said to be symmetric if i and $-i$ belong to the same 2-cyclotomic coset modulo $2^n - 1$). We denote by S_n the set of vectors of length 2^n and of weights $2^{n-1} \pm 2^{\frac{n}{2}-1}$. Then we have the following inclusions ($A \subset B$ means that A is a subcode of B):

$$\mathcal{PS}^{\#}_{ap} = A_n \cap S_n \subset A_n \subset B_n \subset H_n$$

5.4 A characterization of hyper-bentness

Recall that Dillon has exhibited a subclass of $\mathcal{PS}^{-}$, denoted by $\mathcal{PS}_{ap}$, whose elements are defined in an explicit form (see Subsection 4.4.1, Chapter 4). Furthermore, it is well-known (see *e.g.* [36]) that all the functions of $\mathcal{PS}_{ap}$ are hyper-bent.

Youssef and Gong [272] showed that hyper-bent functions actually exist. The following proposition, due to Carlet and Gaborit [36], is an easy translation of this result, which was originally given in terms of sequences, stated using only the terminology of Boolean functions.

Proposition 5.4.1 ($\mathcal{PS}^{\#}_{ap}$ class [272, Theorem 1], [36, Proposition 3])**.** *Let α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$. Then f is a hyper-bent function if and only if the weight of the vector $(f(1), f(\alpha), f(\alpha^2), \cdots, f(\alpha^{2^m}))$ equals 2^{m-1}. In this case f is said to belong to the $\mathcal{PS}^{\#}_{ap}$ class.*

Charpin and Gong [54] have derived a slightly different version of the preceding proposition.

Proposition 5.4.2 ([54, Theorem 2])**.** *Let α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$. Denote by U the cyclic subgroup of $\mathbb{F}^*_{2^n}$ of order $2^m + 1$. Let $\zeta = \alpha^{2^m-1}$ be a generator of U. Then f is a hyper-bent function if and only if the cardinality of the set $\left\{i \mid f(\zeta^i) = 1, 0 \leq i \leq 2^m\right\}$ equals 2^{m-1}.*

Remark 5.4.3. *It is important to point out that bent functions f defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$ are always hyper-bent. A proof of this claim can be found in a paper of Charpin and Gong [54, Proof of Theorem 2] or it can be directly observed that the support $supp(f)$ of such a Boolean function f can be decomposed as $\mathrm{supp}(f) = \bigcup_{i \in S} \alpha^i \mathbb{F}_{2^m}^*$, where $S = \{i \mid f(\alpha^i) = 1\}$, that is, thanks to Theorem 4.4.2, f is bent if and only if $\#S = 2^{m-1}$, proving that such bent functions are actually hyper-bent functions according to Proposition 5.4.1.*

Finally, Carlet and Gaborit have proved the following more precise statement about the functions considered in Proposition 5.4.1.

Proposition 5.4.4 ([36, Proposition 4])**.** *Hyper-bent functions as in Proposition 5.4.1 such that $f(1) = 0$ are the elements of the $\mathcal{PS}_{ap}$ class. Those such that $f(1) = 1$ are elements of $\mathcal{PS}_{ap}^{\#}$ and they are the functions of the form $f(x) = g(\delta x)$ for some $g \in \mathcal{PS}_{ap}$ and $\delta \in \mathbb{F}_{2^n} \setminus \{1\}$ such that $g(\delta) = 1$.*

5.5 Primary constructions and characterization of hyper-bent functions in polynomial forms

5.5.1 Monomial hyper-bent functions via Dillon expnents

Among all the known monomial bent, only the Dillon's function is also hyper-bent. Recall that the monomial Dillon function is the function whose expression is defined with *Dillon exponent* (that is the exponent given in the second row of Table 4.2) as:

$$\forall x \in \mathbb{F}_{2^n}, \quad f_a^{(r)}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}), \quad a \in \mathbb{F}_{2^n}^\star$$

where $m = \frac{n}{2}$ and r is an integer such that $\gcd(r, 2^m + 1) = 1$. The characterization of the bentness of the monomial functions $f_a^{(r)}$ has been studied by Dillon [82] in the case $r = 1$ and, next by Leander [159] (who refined the result of Dillon using a different point of view) and by Charpin and Gong [54] (who extended the family of Dillon, implying in particular that the original functions were actually hyper-bent) for any integer r co-prime with $2^m + 1$. Thanks to these works, the bent and hyper-bent functions $f_a^{(r)}$ have been completely identified. Furthermore, it has been proved that, up to affine equivalence, we can restrict the study of the bentness of $f_a^{(r)}$ to the case where $a \in \mathbb{F}_{2^m}^\star$ (see e.g. [159]). The following theorem summarizes the results related to the bentness of the function $f_a^{(r)}$.

Theorem 5.5.1. *([82, 54]) Let $n = 2m$, $a \in \mathbb{F}_{2^m}^\star$ and $f_a^{(r)}$ be the boolean function defined on $\mathbb{F}_{2^n}$ as follows*

$$\forall x \in \mathbb{F}_{2^n}, \quad f_a^{(r)}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}), \quad \gcd(r, 2^m + 1) = 1.$$

1. *$f_a^{(r)}$ is bent if and only if $f_a^{(1)}$ is bent.*
2. *$f_a^{(1)}$ is bent if and only if $K_m(a) = 0$.*
3. *If $f_a^{(r)}$ is bent then its dual function is $f_a^{(r)}$ itself.*
4. *$f_a^{(r)}$ is hyper-bent if and only if $f_a^{(r)}$ is bent.*
5. *The bent functions $f_a^{(r)}$ are in the Partial Spread class PS_{ap}.*

Remark 5.5.2. *Note that an alternative direct proof of Dillon's result (point 2. of Theorem 5.5.1) has been proposed recently by Leander in [159] (see also [54]). Leander's proof gives also more information on the spectrum of monomial functions $f_{a,0}$. A small mistake in his proof was rectified in [54]). Note also that the existence of some a in $\mathbb{F}_{2^m}$ which are zeros of Kloosterman sum on $\mathbb{F}_{2^m}$ had been conjectured by Dillon. It has been proved by Lachaud and Wolfmann in [156] that the values of such Kloosterman sums are all the numbers divisible by 4 in the range $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$ (which implies in particular that the family defined by Dillon is never empty).*

5.5.2 Binomial hyper-bent functions via Dillon (like) exponents

In the following, we are interested in the problem which consists in finding two exponents s_1 and s_2 with $o(s_2) < n$ and the corresponding coefficients $a \in \mathbb{F}^\star_{2^{o(s_1)}}$ and $b \in \mathbb{F}^\star_{2^{o(s_2)}}$ defining bent or hyper-bent functions defined on $\mathbb{F}_{2^n}$ whose expression is of the form

$$\mathrm{Tr}_1^{o(s_1)}\left(ax^{s_1}\right) + \mathrm{Tr}_1^{o(s_2)}\left(bx^{s_2}\right) \tag{5.2}$$

A first family of binomial hyper-bent functions $\mathfrak{F}_n$

By computer experiments, for small values of n ($n \leq 16$; because of the complexity of the problem), we have found that the set of all functions of type (5.2) with the exponents $s_1 = 3(2^m-1)$ and $s_2 = \frac{2^n-1}{3}$ contains bent functions when m is odd. Note that $o(s_1) = n$ and $o(s_2) = 2$. The polynomial form of a function of type (5.2), denoted by $f_{a,b}$, is then of the form:

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \tag{5.3}$$

where, $a \in \mathbb{F}^\star_{2^{o(s_1)}} = \mathbb{F}^\star_{2^n}$ and $b \in \mathbb{F}^\star_{2^{o(s_2)}} = \mathbb{F}^\star_4$.
Note that when $b = 0$, the corresponding function $f_{a,0}$ is a monomial bent function if and only if a is a zero of Kloosterman sums on $\mathbb{F}_{2^n}$. Denote by $\mathfrak{F}_n$ the set of the Boolean functions $f_{a,b}$ defined on $\mathbb{F}_{2^n}$ whose polynomial form is given by the above expression (5.3). This infinite class is not contained in the class studied by Charpin and Gong [54] that we have mentioned above. In the following, we present the study of bentness of elements of $\mathfrak{F}_n$. To this end, we investigate a precise characterization of such functions of $\mathfrak{F}_n$ which are hyper-bent, by giving explicit conditions on the coefficients a and b. To this end, we show first that $\mathfrak{F}_n$ is a subclass of the well known Partial Spreads class for which the bentness of its functions can be characterized by means of the Hamming weight of their restrictions to a certain set. Next, we investigate the conditions on the choice of a and b for obtaining an explicit family of bent functions. Thanks to the recent works of Charpin, Helleseth and Zinoviev on the Kloosterman sums and cubic sums, we establish an explicit characterization of the bentness of functions belonging to $\mathfrak{F}_n$ in terms of the Kloosterman sums of the coefficient a when m is odd.

The study of the bentness of the binomial family $\mathfrak{F}_n$

• First of all, let us notice that all the functions are of algebraic degree m which is the optimum algebraic degree for a bent function on $\mathbb{F}_{2^n}$ (recall that the algebraic degree of any bent Boolean function on $\mathbb{F}_{2^n}$ is at most m).

Proposition 5.5.3. *([195]) The algebraic degree of any function $f_{a,b}$ of $\mathfrak{F}_n$ is equal to m.*

Proof. The two exponents 2^m-1 and $\frac{2^n-1}{3}$ are of 2-weight m since $2^m-1 = 1+2+2^2+\cdots+2^{m-1}$ and $\frac{2^n-1}{3} = 1+4+\cdots+4^{m-1}$. Therefore, the two Boolean functions $x \mapsto \mathrm{Tr}_1^n(ax^{2^m-1})$ and

$x \mapsto \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ are of algebraic degree equal to m. Since $\mathrm{Tr}_1^n(ax^{2^m-1})$ and $\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ are two separate parts in the trace representation of $f_{a,b}$, the algebraic degree of $f_{a,b}$ is equal to m. □

• Let us note now that all the Boolean functions of the family $\mathfrak{F}_n$ have the following property

$$\forall a \in \mathbb{F}_{2^n}^\star, \quad \forall b \in \mathbb{F}_4, \quad \forall c \in \mathbb{F}_{2^m}^\star, \quad \forall x \in \mathbb{F}_{2^n}, \quad f_{a,b}(c^3x) = f_{a,b}(x). \tag{5.4}$$

That implies in particular that a Boolean function $f_{a,b}$ of $\mathfrak{F}_n$ is constant on each coset of $C = \{x^3 \mid x \in \mathbb{F}_{2^m}^\star\}$. Denote by H a set of representatives for the equivalence relation $\sim$ defined on $\mathbb{F}_{2^n}^\star$ by $x \sim y$ if and only if $y = xv$ for some $v \in C$. Then, we have

$$supp(f_{a,b}) = \bigcup_{x \in S_{a,b}} xC \text{ where } S_{a,b} := \{x \in H \mid f_{a,b}(x) = 1\} \tag{5.5}$$

When m is odd, every element of $\mathbb{F}_{2^m}^\star$ is a cube and thus we have $C = \mathbb{F}_{2^m}^\star$ (indeed, the map $x \in \mathbb{F}_{2^m}^\star \mapsto x^3$ is a permutation for m odd). On the other hand, recall that every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as: $x = yu$, with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U := \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$. Therefore, one can take $H = U$ in this case leading to

$$supp(f_{a,b}) = \bigcup_{u \in S_{a,b}} u\mathbb{F}_{2^m}^\star, \text{ with } S_{a,b} = \{u \in U \mid f_{a,b}(u) = 1\} \tag{5.6}$$

This implies in particular that bent functions belonging to $\mathfrak{F}_n$ are in the Partial Spreads class $\mathcal{PS}$ introduced by Dillon [82]. Therefore, thanks to Theorem 4.4.2, for m odd, the question of deciding whether an element $f_{a,b}$ of $\mathfrak{F}_n$ is bent or not can be reduced to compute the Hamming weight of its restriction to U, that is, we have

Proposition 5.5.4. *([195]) For m odd, the Boolean function $f_{a,b}$ of $\mathfrak{F}_n$ is bent if and only if* $\mathrm{wt}(f_{a,b}|_U) = 2^{m-1}$.

Based on this result, we shall characterize the elements a of $\mathbb{F}_{2^n}$ and $b \in \mathbb{F}_4$ for which $f_{a,b}$ is bent in terms of Kloosterman sum.

• Restriction to the case where $a \in \mathbb{F}_{2^m}^\star$: we are going to show that we can restrict ourselves to study the bentness of $f_{a,b}$ with $a \in \mathbb{F}_{2^m}^\star$ without loss of generality. Let $a \in \mathbb{F}_{2^n}^\star$, $b \in \mathbb{F}_4$, $a' \in \mathbb{F}_{2^m}^\star$ and $b' \in \mathbb{F}_4$. Note that, if $a = a'\lambda^{2^m-1}$ and $b = b'\lambda^{\frac{2^n-1}{3}}$ for some $\lambda \in \mathbb{F}_{2^n}^\star$, the functions $f_{a',b'}$ and $f_{a,b}$ are linearly equivalent. Indeed, one has, for every x in $\mathbb{F}_{2^n}^\star$, $f_{a,b}(x) = f_{a',b'}(\lambda x)$. It follows thus that for our considerations we can always replace $a \in \mathbb{F}_{2^n}^\star$ by the unique element $a' \in \mathbb{F}_{2^m}^\star$ defined by $a = a'u$ where $u \in U = \{\lambda^{2^m-1} \mid \lambda \in \mathbb{F}_{2^n}^\star\}$. In other words, we have

Proposition 5.5.5. *([195, 197]) Let $f_{a,b}$ be a Boolean function whose expression is of the form (5.3). Then,*

$$\begin{aligned}&\{(a,b) \mid a \in \mathbb{F}_{2^n}^\star,\ b \in \mathbb{F}_4,\ f_{a,b} \text{ is bent}\}\\ &\quad = \{(a'\lambda^{2^m-1}, b'\lambda^{\frac{2^n-1}{3}}) \mid a' \in \mathbb{F}_{2^m}^\star, b' \in \mathbb{F}_4, \lambda \in \mathbb{F}_{2^n}^\star, f_{a',b'} \text{ is bent}\}.\end{aligned}$$

Thanks to the previous proposition, one can restrict oneself to the case $a \in \mathbb{F}_{2^m}^\star$ without loss of generality. Proposition 5.5.4 says that for m odd, it suffices to compute the Hamming weight of the restriction to U of $f_{a,b}$, $(a,b) \in \mathbb{F}_{2^m}^\star \times \mathbb{F}_4^\star$, to decide whether $f_{a,b}$ is bent or not. Our aim in this section is to give a necessary and sufficient condition for the bentness of $f_{a,b}$ in terms of

the Kloosterman sum $K_m(a)$. We begin for that by rewording Proposition 5.5.4. To this end, we introduce the following sum

$$\forall (a,b) \in \mathbb{F}_{2^m}^\star \times \mathbb{F}_4^\star, \qquad \Lambda(a,b) := \sum_{u \in U} \chi(f_{a,b}(u)). \tag{5.7}$$

Then, by noting that $\sum_{u\in U} \chi(f_{a,b}(u)) = \#U - 2\,\mathrm{wt}(f_{a,b}|_U) = 2^m + 1 - 2\,\mathrm{wt}(f_{a,b}|_U)$, we have, for every $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$,

$$f_{a,b} \text{ is bent if and only if } \Lambda(a,b) = 1. \tag{5.8}$$

• The key result, that is, that the sum $\Lambda(a,b)$ can be expressed by means of Kloosterman sums and the cubic sums on $\mathbb{F}_{2^m}$ thanks to Proposition 2.3.2

Proposition 5.5.6. *([195, 197]) Let β a primitive element of $\mathbb{F}_4$. Let $a \in \mathbb{F}_{2^m}^\star$. Then we have*

$$\begin{aligned} \Lambda(a,\beta) = \Lambda(a,\beta^2) &= \frac{K_m(a) - 2C_m(a,a) - 1}{3}, \\ \Lambda(a,1) &= \frac{K_m(a) + 4C_m(a,a) - 1}{3}. \end{aligned}$$

Now, thanks to (5.8), Proposition 5.5.6 , Proposition 2.2.5 and Corollary 2.3.3, we are able to identify the values of a for which the Boolean functions $f_{a,1}$, $f_{a,\beta}$ or f_{a,β^2} is bent.

Theorem 5.5.7. *([195, 197]) Let $n = 2m$ be an even integer. Suppose that m is odd, $m > 3$. Let $a \in \mathbb{F}_{2^m}^\star$. Let β be a primitive element of $\mathbb{F}_4$. Let $f_{a,1}$, $f_{a,\beta}$ and f_{a,β^2} be the Boolean functions on $\mathbb{F}_{2^n}$ whose expression is of the form (5.3). If $K_m(a) = 4$ (in this case $\mathrm{Tr}_1^m(a^{1/3}) = 0$),then $f_{a,1}$, $f_{a,\beta}$ and f_{a,β^2} are bent while, if $K_m(a) \neq 4$, then $f_{a,1}$, $f_{a,\beta}$ and f_{a,β^2} are not bent.*

Remark 5.5.8. *For $m = 3$, we have made an exhaustive search of all $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_4^\star$ such that $f_{a,b}$ is bent. We have found that the bent Boolean functions of $\mathfrak{F}_6$ are $f_{1,\beta}$, f_{1,β^2} and every Boolean function $f_{au,b}$ with $b \in \mathbb{F}_4^\star$, $u \in U = \{x \in \mathbb{F}_{2^6}^\star \mid x^9 = 1\}$ and $a \in \mathbb{F}_{2^3}^\star$ such that $K_3(a) = 4$.*

• Now, recall that if a Boolean function f defined on $\mathbb{F}_{2^n}$ is bent then its dual function $\widetilde{f}$ is the Boolean function defined on $\mathbb{F}_{2^n}$ by: $\widehat{\chi_f}(x) = 2^{\frac{n}{2}}\chi(\widetilde{f}(x))$. Moreover, it is well-known that if f is bent then, its dual $\widetilde{f}$ is also bent and that its own dual is f itself.

Proposition 5.5.9. *([197])*

Let $n = 2m$ be an even integer. Suppose that m is odd. Let $f_{a,b}$ ($a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$) be a bent Boolean functions on $\mathbb{F}_{2^n}$ whose expression is of the form (5.3). Then, the dual function of $f_{a,b}$ is equal to $f_{a^{2^m},b^2}$, that is, we have

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{f_{a,b}}}(\omega) = 2^m \chi(f_{a^{2^m},b^2}(\omega)).$$

Proof. Let w be an element of $\mathbb{F}_{2^n}$. Since every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as : $x = yu$, with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U$ we have

$$\widehat{\chi_{f_{a,b}}}(w) := \sum_{x \in \mathbb{F}_{2^n}} \chi(f_{a,b}(x) + \mathrm{Tr}_1^n(wx)) = 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^\star} \chi(f_{a,b}(yu)) + \mathrm{Tr}_1^n(wyu))$$

One has, for m odd, $f_{a,b}(yu) = f_{a,b}(u)$ for every $u \in U$ and $y \in \mathbb{F}_{2^m}^\star$. Thus,

$$\begin{aligned}\widehat{\chi_f}_{a,b}(w) &= 1 - \sum_{u\in U} \chi(f_{a,b}(u)) + \sum_{u\in U} \chi(f_{a,b}(u)) \sum_{y\in\mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^n(wyu)) \\ &= 1 - \sum_{u\in U} \chi(f_{a,b}(u)) + \sum_{u\in U} \chi(f_{a,b}(u)) \sum_{y\in\mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^m(y\,\mathrm{Tr}_m^n(wu))) \\ &= 1 - \sum_{u\in U} \chi(f_{a,b}(u)) + 2^m \sum_{\substack{u\in U \\ \mathrm{Tr}_m^n(wu)=0}} \chi(f_{a,b}(u)).\end{aligned}$$

Note first that $\widehat{\chi_{f_{a,b}}}(0) = 1 - \sum_{u\in U} \chi(f_{a,b}(u)) + 2^m \sum_{u\in U} \chi(f_{a,b}(u))$.
Now, if w is an element of $\mathbb{F}_{2^n}^\star$, then, we have $\mathrm{Tr}_m^n(wu) = 0$ if and only if $uw + u^{2^m} w^{2^m} = 0$, that is, $u^{2^m-1} = w^{1-2^m}$. Then, using the fact that $f_{a,b}(u) = f_{a,b}(w^{-1})$, we obtain

$$\widehat{\chi_f}_{a,b}(w) = 1 - \sum_{u\in U} \chi(f_{a,b}(u)) + 2^m \chi(f_{a,b}(w^{-1})).$$

Moreover, one has $f_{a,b}(w^{-1}) = \mathrm{Tr}_1^n(a\omega^{1-2^m}) + \mathrm{Tr}_1^2(bw^{\frac{1-2^n}{3}}) = \mathrm{Tr}_1^n(a^{2^m}\omega^{2^m-1}) + \mathrm{Tr}_1^2(b(w^{\frac{2^n-1}{3}})^2) = \mathrm{Tr}_1^n(a^{2^m}\omega^{2^m-1}) + \mathrm{Tr}_1^2(b^2 w^{\frac{2^n-1}{3}}) = f_{a^{2^m},b^2}(\omega)$. Hence,

$$\widehat{\chi_f}_{a,b}(w) = 1 - \sum_{u\in U} \chi(f_{a,b}(u)) + 2^m \chi(f_{a^{2^m},b^2}(\omega)) \tag{5.9}$$

Now, recall that according to (5.8), $f_{a,b}$ is bent if and only if $\sum_{u\in U} \chi(f_{a,b}(u)) = 1$. Thus, the result follows. □

Remark 5.5.10. *Note that one can get criterion (5.8) of bentness in terms of $\Lambda(a,b)$ from formula (8.4) that is, without using Dillon's results (Theorem 4.4.2).*

The following theorem summarizes the results presented above related to the bentness of the functions of the family $\mathfrak{F}_n$.

Theorem 5.5.11. *([198]) Let $n = 2m$ with m odd ($m > 3$). Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by*

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

1. *The algebraic degree of $f_{a,b}$ equals m (hence any bent function $f_{a,b}$ has a maximal algebraic degree).*
2. *$f_{a,b}$ is hyper-bent if and only if $f_{a,b}$ is bent.*
3. *$f_{a,b}$ is bent if and only if $K_m(a) = 4$.*
4. *The bent functions $f_{a,b}$ are in the class $\mathcal{PS}^-$ and in the Partial Spread class PS_{ap} if $b = 1$.*
5. *If $f_{a,b}$ is bent then its dual function equals $f_{a^{2^m},b^2}$.*

Remark 5.5.12. *Note that according to [57], the condition $K_m(a) = 4$ (m odd) implies that $a = \frac{c}{(1+c)^4}$ for some c in $\mathbb{F}_{2^m}^\star$.*

Example 5.5.13. *Let $n = 10$. Let us describe the set of bent functions $f_{a,b}$ defined on $\mathbb{F}_{2^{10}}$ of the form $\mathrm{Tr}_1^{10}(ax^{31}) + \mathrm{Tr}_1^2(bx^{341})$ where $a \in \mathbb{F}_{2^{10}}^\star$ and $b \in \mathbb{F}_4^\star$. Let α be a primitive element of $\mathbb{F}_{32} = \mathbb{F}_2(\alpha)$ with $\alpha^5 + \alpha^2 + 1 = 0$. According to table 4 in [56], $E_0 := \{a \in \mathbb{F}_{2^5}^\star, \mathrm{Tr}_1^5(a^{1/3}) = 0\} = \{\alpha^3, \alpha^{21}, \alpha^{14}\}$, $\{a \in \mathbb{F}_{2^5}^\star, K_5(a) = 4\} = \{\alpha^3, \alpha^{21}\}$ and $E_1 := \{a \in \mathbb{F}_{2^5}^\star, \mathrm{Tr}_1^5(a^{1/3}) = 1\} = \{1, \alpha^2, \alpha^9, \alpha^{15}\}$ (recall that, $\mathrm{Tr}_1^5(a^{1/3}) = 1$ implies that $K_5(a) \neq 4$). Then according to Theorem 5.5.11, the functions $f_{\alpha^3,1}$, $f_{\alpha^3,\beta}$, f_{α^3,β^2}, $f_{\alpha^{21},1}$, $f_{\alpha^{21},\beta}$ and f_{α^{21},β^2} are bent while $f_{\alpha^{14},1}$, $f_{\alpha^{14},\beta}$, $f^{(1)}_{\alpha^{14},\beta^2}$, $f_{a,1}, f_{a,\beta}$ and f_{a,β^2} are not bent if $a \in \{1, \alpha^2, \alpha^9, \alpha^{15}\}$. Now, the set $\{(a,b) \mid a \in \mathbb{F}_{2^n}^\star, b \in \mathbb{F}_4, f_{a,b}$ is bent$\}$ is equal to the set $\{(a'\lambda^{2^m-1}, b'\lambda^{\frac{2^n-1}{3}}) \mid a' \in \mathbb{F}_{2^m}^\star, b' \in \mathbb{F}_4, \lambda \in \mathbb{F}_{2^n}^\star, f_{a',b'}$ is bent$\}$. Therefore, we conclude that there exist 198 bent Boolean functions defined over $\mathbb{F}_{2^{10}}$ of the form $\mathrm{Tr}_1^{10}(ax^{31}) + \mathrm{Tr}_1^2(bx^{341})$ (with $b \neq 0$). Such functions are $f_{\alpha^3 u,1}$, $f_{\alpha^3 u,\beta}$, $f_{\alpha^3 u,\beta^2}$, $f_{\alpha^{21}u,1}$, $f_{\alpha^{21}u,\beta}$ and $f_{\alpha^{21}u,\beta^2}$ where u is an element of the group of 33-rd roots of unity of $\mathbb{F}_{2^{10}}$ and β denotes a primitive element of $\mathbb{F}_4$.*

Example 5.5.14. *Let $n = 14$. According to Theorem 5.5.11 and to table 4 in [56], we find that there exist 1161 bent Boolean functions $f_{a,b}$ (with $b \neq 0$) defined over the field $\mathbb{F}_{16384}$ of the form $\mathrm{Tr}_1^{14}(cvx^{127}) + \mathrm{Tr}_1^2(bx^{5461})$ where $c \in \{\alpha^{14}, \alpha^{15}, \alpha^{62}\}$, α is a primitive element of $\mathbb{F}_{128}$ satisfying $\alpha^7 + \alpha^3 + 1 = 0$, v runs through the set of 129-st roots of unity of $\mathbb{F}_{2^{14}}$ and $b \in \{1, \beta, \beta^2\}$ were β is a primitive element of $\mathbb{F}_4$.*

A first family of binomial hyper-bent functions $\mathfrak{F}_n$: a generalization

In the following we show that the characterization of the bentness that we obtained in Subsection 5.5.2 is also valid for functions of more general form $f^{(r)}_{a,b}$ that is of the form

$$f^{(r)}_{a,b}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}) \tag{5.10}$$

where r is co-prime with $2^m + 1$ and with m odd. In fact, Theorem 5.5.11 can be generalized to any r co-prime with $2^m + 1$. and one can show that the bent Boolean function $f^{(r)}_{a,b}$ are also hyper-bent and belong to the Partial Spread class PS_{ap} under some condition on the coefficients a and b. As in the case $r = 1$, one can show that, up to affine equivalence, we can restrict the study of the bentness of $f^{(r)}_{a,b}$ to the case where $a \in \mathbb{F}_{2^m}^\star$.

Theorem 5.5.15. *([198]) Let $n = 2m$ with m odd ($m > 3$). Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$. Let $f^{(r)}_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by (5.10) $f^{(r)}_{a,b}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$*

1. *$f^{(r)}_{a,b}$ is bent if and only if $K_m(a) = 4$.*
2. *$f^{(r)}_{a,b}$ is hyper-bent if and only if $f^{(r)}_{a,b}$ is bent.*
3. *The bent functions $f^{(r)}_{a,b}$ are in the class $\mathcal{PS}^-$. Moreover, the bent functions $f^{(r)}_{a,b}$ are elements of the Partial Spread class $\mathcal{PS}_{ap}$ (resp. $\mathcal{PS}^\#_{ap}$) if $b = 1$ (resp. if $b \neq 1$).*
4. *If $f^{(r)}_{a,b}$ is bent then its dual function equals $f^{(r)}_{a^{2^m},b^2}$.*

Proof. Most of the arguments are similar to those used to prove Theorem 5.5.11. Note that $f^{(r)}_{a,b}$ have the following property:

$$\forall c \in \mathbb{F}_{2^m}^\star, \quad \forall x \in \mathbb{F}_{2^n}, \quad f^{(r)}_{a,b}(c^3 x) = f^{(r)}_{a,b}(x).$$

Indeed (note that $c^{2^m-1}=1$ since $c\in\mathbb{F}_{2^m}^\star$),

$$\begin{aligned}f_{a,b}^{(r)}(c^3x)&=\mathrm{Tr}_1^n\left(a(c^3x)^{r(2^m-1)}\right)+\mathrm{Tr}_1^2\left(b(c^3x)^{\frac{2^n-1}{3}}\right)\\&=\mathrm{Tr}_1^n\left(a(c^{2^m-1})^{3r}x^{r(2^m-1)}\right)+\mathrm{Tr}_1^2\left(b(c^{2^m-1})^{2^m+1}x^{\frac{2^n-1}{3}}\right)=f_{a,b}^{(r)}(x)\end{aligned}$$

That implies in particular that the function $f_{a,b}^{(r)}$ is constant on each coset of $C=\{x^3\mid x\in\mathbb{F}_{2^m}^\star\}$. Denote by H a set of representatives for the equivalence relation $\sim$ defined on $\mathbb{F}_{2^n}^\star$ by $x\sim y$ if and only if $y=xv$ for some $v\in C$. Then, we have $supp(f_{a,b}^{(r)})=\bigcup_{x\in S_{a,b}}xC$ where, $S_{a,b}:=\{x\in H\mid f_{a,b}^{(r)}(x)=1\}$. When m is odd, every element of $\mathbb{F}_{2^m}^\star$ is a cube and thus we have $C=\mathbb{F}_{2^m}^\star$ (indeed, the map $x\in\mathbb{F}_{2^m}^\star\mapsto x^3$ is a permutation for m odd). On the other hand, recall that every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as: $x=yu$, with $y\in\mathbb{F}_{2^m}^\star$ and $u\in U$. Therefore, one can take $H=U$ in this case leading to $supp(f_{a,b}^{(r)})=\bigcup_{u\in S_{a,b}}u\mathbb{F}_{2^m}^\star$, with $S_{a,b}=\{u\in U\mid f_{a,b}^{(r)}(u)=1\}$. This implies, according to Theorem 4.4.2, that $f_{a,b}^{(r)}$ is bent if and only if, $\mathrm{wt}(f_{a,b}^{(r)}|_U)=2^{m-1}$ and that bent functions $f_{a,b}^{(r)}$ are in the well known Partial Spread class $\mathcal{PS}^-$ (which proves the first part of assertion 3)) and that $f_{a,b}^{(r)}$ is bent if and only if $\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))=1$ (since $\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))=\#U-2\,\mathrm{wt}(f_{a,b}^{(r)}|_U)=2^m+1-2\#S_{a,b}$). The assertion 1) is then a direct consequence of Proposition 2.3.2 and Corollary 2.3.3. Now, if α is a primitive element of $\mathbb{F}_{2^n}$ then, $f_{a,b}^{(r)}(\alpha^{2^m+1}x)=f_{a,b}^{(r)}(x)$ for every $x\in\mathbb{F}_{2^n}$ (since 3 divides 2^m+1 when m is odd) and 0 is not in the support of $f_{a,b}^{(r)}$. The conditions of the bentness given by Proposition 5.4.1 are then satisfied. Therefore, $f_{a,b}^{(r)}$ is hyper-bent if and only if $\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))=1$ which proves the assertion 2). The second part of the assertion 3) is a direct application of Proposition 5.4.4. Finally, to compute the dual of a bent function $f_{a,b}^{(r)}$ it suffices to compute the Walsh transform $\widehat{\chi_{f_{a,b}^{(r)}}}(w)$ of $f_{a,b}^{(r)}(w)$ for every $w\in\mathbb{F}_{2^n}$. The calculation of $\widehat{\chi_{f_{a,b}^{(r)}}}(w)$ is analogous to the one of $\widehat{\chi_{f_{a,b}^{(1)}}}(w)$. We include the proof for completeness. Let w be an element of $\mathbb{F}_{2^n}$. Since every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as : $x=yu$, with $y\in\mathbb{F}_{2^m}^\star$ and $u\in U$ we have

$\widehat{\chi_{f_{a,b}^{(r)}}}(w):=\sum_{x\in\mathbb{F}_{2^n}}\chi(f_{a,b}^{(r)}(x)+\mathrm{Tr}_1^n(wx))=1+\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star}\chi(f_{a,b}^{(r)}(yu))+\mathrm{Tr}_1^n(wyu))$.

One has, for m odd, $f_{a,b}^{(r)}(yu)=f_{a,b}^{(r)}(u)$ for every $u\in U$ and $y\in\mathbb{F}_{2^m}^\star$. Thus,

$$\begin{aligned}\widehat{\chi_{f_{a,b}^{(r)}}}(w)&=1-\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))+\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^n(wyu))\\&=1-\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))+\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(y\,\mathrm{Tr}_m^n(wu)))\\&=1-\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))+2^m\sum_{\substack{u\in U\\ \mathrm{Tr}_m^n(wu)=0}}\chi(f_{a,b}^{(r)}(u)).\end{aligned}$$

Note first that $\widehat{\chi_{f_{a,b}^{(r)}}}(0)=1-\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))+2^m\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))$.
Now, if w is an element of $\mathbb{F}_{2^n}^\star$, then, we have $\mathrm{Tr}_m^n(wu)=0$ if and only if $uw+u^{2^m}w^{2^m}=0$, that is, $u^{2^m-1}=w^{1-2^m}$. Then, using the fact that $f_{a,b}^{(r)}(u)=f_{a,b}^{(r)}(w^{-1})$, we obtain

$$\widehat{\chi_{f_{a,b}^{(r)}}}(w)=1-\sum_{u\in U}\chi(f_{a,b}^{(r)}(u))+2^m\chi(f_{a,b}^{(r)}(w^{-1})).$$

Moreover, one has

$$\begin{aligned} f_{a,b}^{(r)}(w^{-1}) &= \mathrm{Tr}_1^n(a\omega^{r(1-2^m)}) + \mathrm{Tr}_1^2(bw^{\frac{1-2^n}{3}}) \\ &= \mathrm{Tr}_1^n(a^{2^m}\omega^{r(2^m-1)}) + \mathrm{Tr}_1^2(b(w^{\frac{2^n-1}{3}})^2) \\ &= \mathrm{Tr}_1^n(a^{2^m}\omega^{r(2^m-1)}) + \mathrm{Tr}_1^2(b^2w^{\frac{2^n-1}{3}}) \\ &= f_{a^{2^m},b^2}^{(r)}(\omega). \end{aligned}$$

Hence, $\widehat{\chi_{f_{a,b}^{(r)}}}(w) = 1 - \sum_{u\in U}\chi(f_{a,b}^{(r)}(u)) + 2^m\chi(f_{a^{2^m},b^2}^{(r)}(\omega))$. Now, recall that we have seen that $f_{a,b}^{(r)}$ is bent if and only if $\sum_{u\in U}\chi(f_{a,b}^{(r)}(u)) = 1$. Thus, the assertion 4) follows. □

A first family of binomial hyper-bent functions $\mathfrak{F}_n$: a special case

In this subsection, we focus on the functions $f_{a,b}$ of the family $\mathfrak{F}_n$ or more generally on functions of the form $f_{a,b}^{(r)}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ in the case where m is even. (in this case, 3 divides 2^m-1). By exhaustive search, we find that the family $\mathfrak{F}_n$ contains bent functions for larger values of $m \geq 2$. We shall discus the computational point of view in Section 5.5.2. From now on we therefore assume that $m \geq 2$. In the following we are interested to treat the even case in theoretical point of view.
We have seen in Subsection 5.5.2 that all the Boolean functions of the family $\mathfrak{F}_n$ of the form : have the following property

$$\forall a \in \mathbb{F}_{2^n}^\star, \quad \forall b \in \mathbb{F}_4, \quad \forall c \in \mathbb{F}_{2^m}^\star, \quad \forall x \in \mathbb{F}_{2^n}, \quad f_{a,b}(c^3x) = f_{a,b}(x). \tag{5.11}$$

That implies in particular that a Boolean function $f_{a,b}$ of $\mathfrak{F}_n$ is constant on each coset of $C = \{x^3 \mid x \in \mathbb{F}_{2^m}^\star\}$. Denote by H a set of representatives for the equivalence relation $\sim$ defined on $\mathbb{F}_{2^n}^\star$ by $x \sim y$ if and only if $y = xv$ for some $v \in C$. Then, we have

$$supp(f_{a,b}) = \bigcup_{x\in S_{a,b}} xC \text{ where } S_{a,b} := \{x \in H \mid f_{a,b}(x) = 1\} \tag{5.12}$$

We have seen that when m is odd, $C = \mathbb{F}_{2^m}^\star$ and one can take $H = U$. Let us now consider the case where m is even. In this case, one has $C \neq \mathbb{F}_{2^m}^\star$. Now, unlike in the odd case, a Boolean function $f_{a,b}$ is not constant on any coset $u\mathbb{F}_{2^m}^\star$, $u \in U$, of $\mathbb{F}_{2^m}^\star$. Indeed, for every $y \in \mathbb{F}_{2^m}^\star$, we have

$$f_{a,b}(uy) = \mathrm{Tr}_1^n(au^{2^m-1}) + \mathrm{Tr}_1^2(by^{\frac{2^n-1}{3}}) \tag{5.13}$$

because $\frac{2^n-1}{3}$ is a multiple of 2^m+1 for m even. The algebraic degree of the restriction of $f_{a,b}$ to $u\mathbb{F}_{2^m}^\star$ is hence equal to the 2-weight of $\frac{2^n-1}{3}$, that is, equal to m. The situation seems then to be more complicated that in the odd case since the support of $f_{a,b}$ is not of the form (5.6), that is, the study of the bentness of $f_{a,b}$ cannot be done as in the Subsection 5.5.2. In particular, it is difficult to answer the question of knowing if a function $f_{a,b}$ is or not in the Partial Spreads class. But nevertheless, in this case, we succeed in establishing in the Theorem 5.5.16 a necessary condition expressed in terms of Kloosterman sum that an element a has to satisfy so that the function $f_{a,b}$ is bent.

Theorem 5.5.16. *([197]) Let $f_{a,b} \in \mathfrak{F}_n$, with $a \in \mathbb{F}_{2^m}^\star$, $m \geq 2$ even and $b \in \mathbb{F}_4^\star$. Then, a function $f_{a,b}$ is bent only if $K_m(a) = 4$.*

In fact the result given in Theorem 5.5.16 can be extended for functions $f_{a,b}^{(r)}$ of the form (5.10) (for any integer r co-prime with 2^m+1) as follows.

Theorem 5.5.17. *([198]) Let $n = 2m$ with m even ($m \geq 2$). Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$. Let $f_{a,b}^{(r)}$ be the function defined on $\mathbb{F}_{2^n}$ by $f_{a,b}^{(r)}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$. If $f_{a,b}^{(r)}$ is bent then, $K_m(a) = 4$.*

Proof. Recall that $f_{a,b}^{(r)}$ is bent if and only if $\widehat{\chi_{f_{a,b}^{(r)}}}(w) = \pm 2^m$ for every $w \in \mathbb{F}_{2^n}$. In particular, if $f_{a,b}^{(r)}$ is bent then, we should have $\widehat{\chi_{f_{a,b}^{(r)}}}(0) = \pm 2^m$. Recall that every non-zero element x of $\mathbb{F}_{2^n}$ has a unique decomposition as: $x = yu$ with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U$. Then, the Walsh transform of $f_{a,b}^{(r)}$ at 0 is given by (we use the fact that $y^{2^m-1} = 1$ and $u^{\frac{2^n-1}{3}} = 1$, since 3 divides $2^m - 1$ when m is even):

$$\begin{aligned}\widehat{\chi_{f_{a,b}^{(r)}}}(0) &= \sum_{x\in\mathbb{F}_{2^n}} \chi(f_{a,b}^{(r)}(x)) = 1 + \sum_{x\in\mathbb{F}_{2^n}^\star} \chi(f_{a,b}^{(r)}(x)) \\ &= 1 + \sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) \sum_{y\in\mathbb{F}_{2^m}^\star} \chi(\mathrm{Tr}_1^2(by^{\frac{2^n-1}{3}})).\end{aligned}$$

Split $\mathbb{F}_{2^m}^\star$ as $\mathbb{F}_{2^m}^\star = C' \cup \beta C' \cup \beta^2 C'$ where C' the set of the cubic elements of $\mathbb{F}_{2^m}^\star$ and β is an element of $\mathbb{F}_{2^m} \setminus C'$. We thus get

$$\widehat{\chi_{f_{a,b}^{(r)}}}(0) = 1 + \sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) \sum_{i=0}^{2} \sum_{z\in C'} \chi(\mathrm{Tr}_1^2(b(z\beta^i)^{\frac{2^n-1}{3}})).$$

Since z is a cube of an element of $\mathbb{F}_{2^m}^\star$ we have,

$$\begin{aligned}\sum_{i=0}^{2} \sum_{z\in C'} \chi(\mathrm{Tr}_1^2(b(z\beta^i)^{\frac{2^n-1}{3}})) &= \sum_{i=0}^{2} \sum_{z\in C'} \chi(\mathrm{Tr}_1^2(b\beta^{i\frac{2^n-1}{3}})) \\ &= \sum_{z\in C'} \sum_{\tau\in\mathbb{F}_4^\star} \chi(\mathrm{Tr}_1^2(\tau)) = \sum_{z\in C'} \Big(\sum_{\tau\in\mathbb{F}_4} \chi(\mathrm{Tr}_1^2(\tau)) - 1 \Big) \\ &= -\#C' = -\frac{2^m-1}{3}.\end{aligned}$$

On the other hand, the map $u \mapsto u^r$ is a permutation of U (since $\gcd(r, 2^m + 1) = 1$) and the map $u \mapsto u^{2^m-1}$ is also a permutation of U . Hence, using the well known result, that is $\sum_{u\in U} \chi(\mathrm{Tr}_1^n(au)) = 1 - K_m(a)$, we obtain, $\sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) = \sum_{u\in U} \chi(\mathrm{Tr}_1^n(au)) = 1 - K_m(a)$. We thus deduce

$$\widehat{\chi_{f_{a,b}^{(r)}}}(0) = 1 + \frac{2^m-1}{3}(K_m(a) - 1).$$

Now, if $f_{a,b}^{(r)}$ is bent, then one has necessarily $1 + \frac{2^m-1}{3}(K_m(a) - 1) = \pm 2^m$, that is, $K_m(a) = 4$ or $(2^m - 1)(K_m(a) - 1) = -3(2^m + 1)$. The second equality being impossible since $2^m - 1$ and $2^m + 1$ are co-prime, this proves the result. □

Note that according to [57], the condition $K_m(a) = 4$ (m even) implies that $a = c^3$ for some c such that $\mathrm{Tr}_2^m(c) \neq 0$. The previous Theorem enable one to exhibit an infinite family of functions of type (5.10) which are not bent. Moreover, one can prove that the study of the bentness of $f_{a,b}^{(r)}$ can be reduced to the case where $b = 1$.

Proposition 5.5.18. *([198]) Let $n = 2m$ with m even ($m \geq 2$). Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$. Let $f_{a,b}^{(r)}$ be the function defined on $\mathbb{F}_{2^n}$ by (5.10). Then, $f_{a,b}^{(r)}$ is bent if and only if, $f_{a,1}^{(r)}$ is bent.*

Proof. Since m is even, $\mathbb{F}_4^\star \subset \mathbb{F}_{2^m}^\star$. In particular, for every $b \in \mathbb{F}_4^\star$, there exists $\alpha \in \mathbb{F}_{2^m}^\star$ such that $\alpha^{\frac{2^n-1}{3}} = b$. For $x \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} f_{a,b}^{(r)}(x) &:= \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}) \\ &= \mathrm{Tr}_1^n(a(\alpha^{2^m-1})^r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(\alpha^{\frac{2^n-1}{3}} x^{\frac{2^n-1}{3}}) \\ &= \mathrm{Tr}_1^n(a(\alpha x)^{r(2^m-1)}) + \mathrm{Tr}_1^2((\alpha x)^{\frac{2^n-1}{3}}) \\ &= f_{a,1}^{(r)}(\alpha x). \end{aligned}$$

Hence, for every $\omega \in \mathbb{F}_{2^n}^\star$, we have

$$\begin{aligned} \widehat{\chi_{f_{a,b}^{(r)}}}(\omega) &= \sum_{x \in \mathbb{F}_{2^n}} \chi(f_{a,b}^{(r)}(x) + \mathrm{Tr}_1^n(\omega x)) \\ &= \sum_{x \in \mathbb{F}_{2^n}} \chi(f_{a,1}^{(r)}(\alpha x) + \mathrm{Tr}_1^n(\omega x)) \\ &= \widehat{\chi_{f_{a,1}^{(r)}}}(\omega\alpha^{-1}) \end{aligned}$$

□

The exact value of the Walsh transform $\widehat{\chi_{f_{a,1}^{(r)}}}(\omega)$ of $f_{a,1}^{(r)}$ seems difficult to compute. Nevertheless, we give in the following an expression of $\widehat{\chi_{f_{a,1}^{(r)}}}(\omega)$ for every element ω of $\mathbb{F}_{2^n}^\star$.

Proposition 5.5.19. *([198]) Let $n = 2m$ with m even. Let $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$. Then for every $\omega \in \mathbb{F}_{2^n}^\star$, we have*
$\widehat{\chi_{f_{a,1}^{(r)}}}(\omega) = \frac{2}{3}\sum_{u \in U}\sum_{y \in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(\omega uy^3)) - 2^m\chi(\mathrm{Tr}_1^n(a\omega^{r(1-2^m)}))$.

Proof. Recall that every non-zero element x of $\mathbb{F}_{2^n}$ has a unique decomposition as: $x = yu$ with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U$. Since $y^{2^m-1} = 1$ and $u^{\frac{2^n-1}{3}} = 1$ (because 3 divides $2^m - 1$ when m is even), we have for every $\omega \in \mathbb{F}_{2^n}$

$$\begin{aligned} \widehat{\chi_{f_{a,1}^{(r)}}}(\omega) &= \sum_{x \in \mathbb{F}_{2^n}} \chi(\mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(x^{\frac{2^n-1}{3}}) + \mathrm{Tr}_1^n(wx)) \\ &= 1 + \sum_{u \in U}\sum_{y \in \mathbb{F}_{2^m}^\star} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^2(y^{\frac{2^n-1}{3}}) + \mathrm{Tr}_1^n(wuy)). \end{aligned}$$

Now, $\mathrm{Tr}_1^2(y^{\frac{2^n-1}{3}}) = 0$ if and only if $y \in C' := \{y^3,\ y \in \mathbb{F}_{2^m}^\star\}$. Then, $\widehat{\chi_{f_{a,1}^{(r)}}}(\omega)$

$$\begin{aligned}
&= 1 + \sum_{u\in U}\sum_{y\in C'} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) \\
&\quad - \sum_{u\in U}\sum_{y\notin C'} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) \\
&= 1 + 2\sum_{u\in U}\sum_{y\in C'} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) \\
&\quad - \sum_{u\in U}\sum_{y\in \mathbb{F}_{2^m}^\star} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) \\
&= 1 + 2\sum_{u\in U}\sum_{y\in C'} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) \\
&\quad + \sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) \\
&\quad - \sum_{u\in U}\sum_{y\in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy))
\end{aligned}$$

Firstly, the maps $x \mapsto x^{2^m-1}$ and $x \mapsto x^r$ being permutations of U (since $\gcd(r, 2^m+1) = 1$) hence, $\sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) = \sum_{u\in U} \chi(\mathrm{Tr}_1^n(au)) = 1 - K_m(a)$. Secondly,

$$\begin{aligned}
&\sum_{u\in U}\sum_{y\in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) \\
&= \sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) \sum_{y\in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^n(wuy))).
\end{aligned}$$

Using the transitivity rule of trace function, we obtain

$$\begin{aligned}
&\sum_{u\in U}\sum_{y\in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) \\
&= \sum_{u\in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) \sum_{y\in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\omega u)y)).
\end{aligned}$$

But $\sum_{y\in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\omega u)y))$

$$= \begin{cases} 2^m & \text{if } \mathrm{Tr}_m^n(\omega u) = 0, \text{ that is, if } u^{2^m-1} = \omega^{1-2^m} \\ 0 & \text{otherwise} \end{cases}$$

Hence, $\sum_{u\in U}\sum_{y\in \mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^n(wuy)) = 2^m \chi(\mathrm{Tr}_1^n(a\omega^{r(1-2^m)}))$.

Moreover, $\sum_{u\in U}\sum_{y\in C'}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^n(wuy))$

$$\begin{aligned}
&= \frac{1}{3}\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})\\
&\quad +\mathrm{Tr}_1^n(\omega uy^3))\\
&= \frac{1}{3}\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})\\
&\quad +\mathrm{Tr}_1^n(\omega uy^3))-\frac{1}{3}\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))\\
&= \frac{1}{3}\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^n(\omega uy^3))\\
&\quad +\frac{1}{3}K_m(a)-\frac{1}{3}.
\end{aligned}$$

Collecting the previous calculations, we obtain $\widehat{\chi_{f_{a,1}^{(r)}}}(\omega)$

$$\begin{aligned}
&= \frac{1}{3}(4-K_m(a))+\frac{2}{3}\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})\\
&\quad +\mathrm{Tr}_1^n(\omega uy^3))-2^m\chi(\mathrm{Tr}_1^n(a\omega^{r(1-2^m)})).
\end{aligned}$$

The result follows if $K_m(a)$ equals 4. □

Remark 5.5.20. *Let $n=2m$ with m even. Let $a\in\mathbb{F}_{2^m}^\star$. For every $\omega\in\mathbb{F}_{2^n}^\star$, we have*

$$\sum_{b\in\mathbb{F}_4^\star}\widehat{\chi_{f_{a,b}^{(1)}}}(\omega)=4-K_m(a)-2^m\chi(\mathrm{Tr}_1^n(a\omega^{2^m-1}))$$

In particular, $\sum_{b\in\mathbb{F}_4}\widehat{\chi_{f_{a,b}^{(1)}}}(\omega)=4$. Indeed, every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as: $x=yu$, with $y\in\mathbb{F}_{2^m}^\star$ and $u\in U$. Hence, for every $\omega\in\mathbb{F}_{2^n}^\star$ we have $\sum_{b\in\mathbb{F}_4^\star}\widehat{\chi_{f_{a,b}^{(1)}}}(\omega)$

$$\begin{aligned}
&= \sum_{x\in\mathbb{F}_{2^n}}\chi(\mathrm{Tr}_1^n(ax^{2^m-1}+\omega x))\sum_{b\in\mathbb{F}_4^\star}\chi(\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}))\\
&= 3-\sum_{x\in\mathbb{F}_{2^n}^\star}\chi(\mathrm{Tr}_1^n(ax^{2^m-1}+\omega x))\\
&= 3-\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{2^m-1}))\sum_{y\in\mathbb{F}_{2^m}^\star}\chi(\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\omega u)y))\\
&= 4-K_m(a)-\\
&\quad \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{2^m-1}))\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\omega u)y))
\end{aligned}$$

The previous equality follows from the well known result, that is $\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au))=1-K_m(a)$. Now, $\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\omega u)y))$

$$=\begin{cases}2^m & \text{if } \mathrm{Tr}_m^n(\omega u)=0, \text{ that is, if } u^{2^m-1}=\omega^{1-2^m}\\ 0 & \text{otherwise}\end{cases}$$

Thus, $\sum_{b\in\mathbb{F}_4^\star}\widehat{\chi_{f_{a,b}^{(1)}}}(\omega) = 4 - K_m(a) - 2^m\chi(\mathrm{Tr}_1^n(a\omega^{1-2^m}))$.

Now, according to [159],

$$\forall\omega\in\mathbb{F}_{2^n}, \widehat{\chi_{f_{a,0}^{(1)}}}(\omega) = 2^m\chi(\mathrm{Tr}_1^n(a\omega^{2^m-1})) + K_m(a).$$

Hence, $\sum_{b\in\mathbb{F}_4}\widehat{\chi_{f_{a,b}^{(1)}}}(\omega) = 4$.

• Experimental results for m even:

The functions that we have introduced in [197] are defined for $a\in\mathbb{F}_{2^m}^*$ and $b\in\mathbb{F}_4^*$ as the Boolean functions $f_{a,b}$ with $n=2m$ inputs given by

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \ . \tag{5.14}$$

When m is even, we have shown that the situation seems to be more complicated theoretically than in the case where m is odd, and that the study of the bentness cannot be done as in the odd case. Here, we only have a necessary condition to build bent functions from the value 4 of binary Kloosterman sum when m is even. To get a better understanding of the situation we conducted some experimental investigations to check whether the Boolean functions constructed with the formula (5.14) were bent or not for all the a's in $\mathbb{F}_{2^m}$ giving a Kloosterman sum with value 4.

First, we show that it is enough to study the bentness of a subset of these functions to get results about all of them.

First of all, the next proposition proves that the study of the bentness of $f_{a,b}$ can be reduced to the case where $b=1$.

Proposition 5.5.21. *Let $n=2m$ with $m\geq 2$ even. Let $a\in\mathbb{F}_{2^m}^*$ and $b\in\mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by Equation* (5.14)*. Then $f_{a,b}$ is bent if and only if $f_{a,1}$ is bent.*

Proof. Since m is even, we have the inclusion of fields $\mathbb{F}_4^*\subset\mathbb{F}_{2^m}^*$. In particular, for every $b\in\mathbb{F}_4^*$, there exists $\alpha\in\mathbb{F}_{2^m}^*$ such that $\alpha^{\frac{2^n-1}{3}} = b$. For $x\in\mathbb{F}_{2^n}$, we have

$$\begin{aligned} f_{a,b}(x) &= \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_1^n\left(a\alpha^{2^m-1}x^{2^m-1}\right) + \mathrm{Tr}_1^2\left(\alpha^{\frac{2^n-1}{3}}x^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_1^n\left(a(\alpha x)^{2^m-1})\right) + \mathrm{Tr}_1^2\left((\alpha x)^{\frac{2^n-1}{3}}\right) \\ &= f_{a,1}(\alpha x) \ . \end{aligned}$$

Hence, for every $\omega\in\mathbb{F}_{2^n}^*$, we have

$$\begin{aligned} \widehat{\chi_{f_{a,b}}}(\omega) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{f_{a,b}(x)+\mathrm{Tr}_1^n(\omega x)} \\ &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{f_{a,1}(\alpha x)+\mathrm{Tr}_1^n(\omega x)} \\ &= \widehat{\chi_{f_{a,1}}}(\omega\alpha^{-1}) \ . \end{aligned}$$

□

Second, we know that $K_m(a) = K_m(a^2)$, so the a's in $\mathbb{F}_{2^m}$ giving binary Kloosterman sums with value 4 come in cyclotomic classes. Fortunately, it is enough to check one a per class. Indeed, $f_{a,b}$ is bent if and only if f_{a^2,b^2} is, as proved in the following proposition.

Proposition 5.5.22. *Let $n = 2m$ with $m \geq 2$ even. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by Equation* (5.14)*. Then $f_{a,b}$ is bent if and only if f_{a^2,b^2} is bent.*

Proof.

$$\begin{aligned}
\widehat{\chi_{f_{a,b}}}(\omega) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a,b}(x)+\mathrm{Tr}_1^n(\omega x)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n(\omega x)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(a^2x^{2^{2^m-1}}\right)+\mathrm{Tr}_1^2\left(b^2x^{2\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n\left(\omega^2x^2\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(a^2x^{2^m-1}\right)+\mathrm{Tr}_1^2\left(b^2x^{\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n\left(\omega^2x\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a^2,b^2}(x)+\mathrm{Tr}_1^n\left(\omega^2x\right)} \\
&= \widehat{\chi_{f_{a^2,b^2}}}(\omega^2) \ .
\end{aligned}$$

□

In the specific case $b = 1$ that we are interested in, it gives that $f_{a,1}$ is bent if and only if $f_{a^2,1}$ is, which proves that checking one element of each cyclotomic class is enough.

Finally, as mentioned in Section 7.4.2, finding all the a's in $\mathbb{F}_{2^m}$ giving a specific value is a different problem from finding one such $a \in \mathbb{F}_{2^m}$. One can compute the Walsh–Hadamard transform of the trace of the inverse function using a fast Walsh–Hadamard transform. As long as the basis of $\mathbb{F}_{2^m}$ considered as a vector space over $\mathbb{F}_2$ is correctly chosen so that the trace corresponds to the scalar product, the implementation is straightforward.

The algorithm that we implemented is described in Algorithm 5.1.

Algorithm 5.1: Testing bentness for m even

Input: An even integer $m \geq 2$
Output: A list of couples made of one representative for each cyclotomic class of elements $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$ together with 1 if the corresponding Boolean functions $f_{a,b}$ are bent, 0 otherwise

```
Build the Boolean function f : x ∈ F_{2^n} ↦ Tr_1^n(1/x) ∈ F_2
Compute the Walsh–Hadamard transform of f
Build a list A made of one a ∈ F_{2^m} for each cyclotomic class such that K_m(a) = 4
Initialize an empty list R
foreach a ∈ A do
    Build the Boolean function f_{a,1}
    Compute the Walsh–Hadamard transform of f_{a,1}
    if f_{a,1} is bent then
        Append (a, 1) to R
    else
        Append (a, 0) to R
return R
```

The implementation was made using Sage [241] and Cython [9], performing direct calls to Givaro [96], NTL [235] and gf2x [10] libraries for efficient manipulation of finite field elements and construction of Boolean functions.

In Table 5.1 we give the results of the computations we conducted along with different pieces of information about them. One should remark that all the Boolean functions which could be tested are bent.

Table 5.1 – Test of bentness for m even

m	Nb. of cyclotomic classes	Time	All bent?
4	1	<1s	yes
6	1	<1s	yes
8	2	<1s	yes
10	3	4s	yes
12	6	130s	yes
14	8	3000s	yes
16	14	82000s	yes
18	20	-	-
20	76	-	-
22	87	-	-
24	128	-	-
26	210	-	-
28	810	-	-
30	923	-	-
32	2646	-	-

Evidence that our computations were correct is given by the fact that the number of cyclotomic classes we found is so. This can be checked using the formula of Proposition 7.1.4. We are looking for elliptic curves with trace t of the Frobenius endomorphism equal to $t = 1 - K_m(a) = -3$. Hence, the number of cycloctomic classes is $H(\Delta)/m$ where $H(\Delta)$ is the Kronecker class number and $\Delta = 9 - 4 \cdot 2^m$. Moreover, for the values we tested, except $m = 12, 30, 32$, this discriminant is fundamental, so that the order $\mathbb{Z}[\alpha]$ is maximal and $H(\Delta) = h(\Delta)$ the classical class number, a quantity even easier to compute.

Unfortunately, we were not able to check bentness of functions for $m > 16$ due to lack of memory. Constructing the Boolean functions in $n = 2m$ variables is the most time consuming part of the test, but the real bottleneck is the amount of memory needed to compute their Walsh–Hadamard transforms. One must indeed perform these computations using integers of size at least $2m + 1$ bits, so, with our implementation, integers of 64 bits as soon as $m \geq 16$. The amount of memory needed is then $64 \cdot 2^{2m} \cdot 2^{-30} = 2^{2m-24}$ GB. For $m = 16$ this represents already 32 GB of memory; for $m = 18$ it would be 512 GB of memory. Therefore, we give in Table 5.2 the fourteen values of a found for $m = 16$, the highest value that we could test. In this table the finite field $\mathbb{F}_{2^{16}}$ is represented as $\mathbb{F}_2[x]/(x^{16} + x^5 + x^3 + x^2 + 1)$. The corresponding Boolean functions in $n = 32$ variables are all bent as we already pointed out.

Finally, we give some open questions: :

Question 5.5.23.

Assume m even. Does a bent function $f_{a,b}^{(r)}$ of the form 5.10 belong to the Partial spread class PS^- ?

Table 5.2 – The fourteen cyclotomic classes such that $K_{16}(a) = 4$ as elements of $\mathbb{F}_2[x]/(x^{16} + x^5 + x^3 + x^2 + 1)$

$$
\begin{array}{l}
x^{14} + x^{11} + x^8 + x^6 + x^3 + x \\
x^{15} + x^{13} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1 \\
x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^2 + x \\
x^{14} + x^{12} + x^{11} + x^9 + x^6 + x \\
x^{15} + x^{11} + x^9 + x^7 + x^6 + x^3 + x^2 + 1 \\
x^{13} + x^6 + x^4 + x^2 + x + 1 \\
x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^3 + x^2 + x \\
x^{15} + x^{11} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 \\
x^{15} + x^{13} + x^9 + x^8 + x^5 + x^4 + x^3 + x \\
x^{15} + x^{11} + x^{10} + x^3 \\
x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x \\
x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x \\
x^{15} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^5 + x \\
x^{15} + x^{11} + x^{10} + x^3 + x + 1
\end{array}
$$

Question 5.5.24.

Assume m even. Are the bent functions $f_{a,b}^{(r)}$ of the from 5.10 also hyper-bent ?

If the answer to Question 5.5.23 is "no" and the one to Question 5.5.24 is "yes" then, we will obtain for the first time a family of hyper-bent functions which are not in the class PS^-. Such functions do not exist in the literature.

A second family of binomial hyper-bent functions $\mathfrak{G}_n$

By computer experiments, for small values of n ($n \leq 14$; because of the complexity of the problem), we have found that the set of all functions of type (5.2) with the exponents $s_1 = 3(2^m - 1)$ and $s_2 = \frac{2^n-1}{3}$ contains bent functions. Note that $o(s_1) = n$ and $o(s_2) = 2$. The polynomial form of a function of type (5.2), denoted by $g_{a,b}$, is then of the form:

$$g_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \tag{5.15}$$

where, $a \in \mathbb{F}^\star_{2^{o(s_1)}} = \mathbb{F}^\star_{2^n}$ and $b \in \mathbb{F}^\star_{2^{o(s_2)}} = \mathbb{F}^\star_4$.
Note that when $b = 0$, the function $g_{a,0}$ is never bent. Moreover, we only treat the case where m is odd since when m is even, s_1 is a Dillon exponent (since $\gcd(3, 2^m + 1) = 1$ if m is even), that is, a case studied previously. In addition, by computer experiments, we have found that there exist no bent functions for n less than 16 with m even. Therefore, in the following, we assume in this subsection m iodd.

Denote by $\mathfrak{G}_n$ the set of the Boolean functions $g_{a,b}$ defined on $\mathbb{F}_{2^n}$ whose polynomial form is given by the above expression (5.15). This infinite class is not contained in the class of functions $\mathfrak{F}_n$ studied in Subsection 5.5.2 (since 3 is a divisor of $2^m + 1$ (m being odd)) nor in the class studied by Charpin and Gong [54] that we have mentioned above. In the following, we present the study of bentness of elements of $\mathfrak{G}_n$. To this end, we investigate a precise characterization of such functions of $\mathfrak{G}_n$ which are hyper-bent, by giving explicit conditions on the coefficients a and b. We firstly show that one can restrict oneself to study the bentness for some particular forms of functions belonging to $\mathfrak{G}_n$ (Lemma 8.1.10). Afterwards, we show that $\mathfrak{G}_n$ is a subclass of the

well known Partial Spreads class for which the bentness of its functions can be characterized by means of the Hamming weight of their restrictions to a certain set (Lemma 5.5.28). We show in Proposition 5.5.29 that bent functions of the class $\mathfrak{G}_n$ are also hyper-bent and more precisely, are (up to a linear transformation) elements of the $\mathcal{PS}_{ap}$ class. We prove in Proposition 5.5.31 and Proposition 5.5.32 that, deciding whether an element of $\mathfrak{G}_n$ is bent or not, depends strongly on the Kloosterman sums and also (in some cases) on the cubic sums involving only the coefficient a. Theorem 5.5.35 recapitulates the results of our study in which we prove that the class $\mathfrak{G}_n$ contains hyper-bent functions when $m \not\equiv 3 \pmod 6$ while, there is no hyper-bent functions in this class when $m \equiv 3 \pmod 6$; an important point is that this class does not contains other bent functions except those which are hyper-bent. Finally, we show that a bent function of the class $\mathfrak{G}_n$ is normal and we compute its dual function.

The study of the bentness of the binomial family $\mathfrak{G}_n$

• First let compute the algebraic degree of functions in $\mathfrak{G}_n$.

Proposition 5.5.25. *([196]) The elements $g_{a,b}$ of $\mathfrak{G}_n$ are all of algebraic degree m.*

Proof. Note that the 2-weights of $3(2^m-1)$ and $\frac{2^n-1}{3}$ are both equal to m (since $3(2^m-1) = 1+2^2+2^3+\cdots+2^{m-1}+2^{m+1}$ and $\frac{2^n-1}{3} = 1+4+\cdots+4^{m-1}$). Thus, the two Boolean functions $x \mapsto \mathrm{Tr}_1^n(ax^{3(2^m-1)})$ and $x \mapsto \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ are of algebraic degree equal to m. The trace functions $\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right)$ and $\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ are two separate parts in the trace representation of $g_{a,b}$, the algebraic degree of $g_{a,b}$ is then equal to m. □

Recall that the algebraic degree of any bent Boolean function on $\mathbb{F}_{2^n}$ is at most m (in the case that $n=2$, the bent functions have degree 2). Bent functions of $\mathfrak{G}_n$ are then of maximum algebraic degree.

Remark 5.5.26. *Recall that an integer d is called a bent exponent if there exists $a \in \mathbb{F}_{2^n}^\star$ for which the function $x \mapsto \mathrm{Tr}_1^n(ax^d)$ is bent. Now, recall that if an integer d is a bent exponent then, either* $\gcd(d, 2^m-1) = 1$ *or* $\gcd(d, 2^m+1) = 1$ *, where $m = n/2$ (see for instance [159]). Consequently, unlike the functions $\mathfrak{F}_n$ presented above ([195, 197]), the monomial functions of the class $\mathfrak{G}_n$ (case $b = 0$) are never bent since the exponent $d = 3(2^m-1)$ is not co-prime with 2^m-1 nor with 2^m+1 (because when m is odd then 3 divides 2^m+1).*

• Now, recall (see Section 4.1, Chapter 4) that if f and f' are two n-variable Boolean functions such that f' is linearly equivalent to f (that is, there exists an $\mathbb{F}_2$-linear automorphism L of $\mathbb{F}_{2^n}$ such that $f' = f \circ L$) then, f is bent if and only if f' is bent.

Let $a \in \mathbb{F}_{2^m}^\star$, $\lambda \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_4^\star$. Set $a' = a\lambda^{3(2^m-1)}$ and $b' = b\lambda^{\frac{2^n-1}{3}}$. Then we remark that, for every $x \in \mathbb{F}_{2^n}$, we have:

$$g_{a',b'}(x) \quad = \quad \mathrm{Tr}_1^n(a(\lambda x)^{3(2^m-1)}) + \mathrm{Tr}_1^2(b(\lambda x)^{\frac{2^n-1}{3}}) = g_{a,b}(\lambda x) \tag{5.16}$$

This means that $g_{a',b'}$ is linearly equivalent to $g_{a,b}$. Consequently, we are not obliged to consider all the possible values of $a \in \mathbb{F}_{2^n}$ in our study of the bentness of an element of $\mathfrak{G}_n$. Indeed, recall that every element of x in $\mathbb{F}_{2^n}^\star$ admits a unique polar decomposition $x = uy$ where $y \in \mathbb{F}_{2^m}^\star$ and $u \in U := \{u \in \mathbb{F}_{2^n}^\star \mid u^{2^m+1} = 1\}$. Now, m being odd, one can decompose U as follows

$$U = V \cup \zeta V \cup \zeta^2 V \tag{5.17}$$

where $V = \{u^3 \mid u \in U\}$ and $\zeta = \xi^{2^m-1}$ where ξ denotes a primitive element of the field $\mathbb{F}_{2^n}$. Thus, every element $u \in U$ can be uniquely decomposed as $u = \zeta^i v$ with $i \in \{0,1,2\}$ and $v \in V$. Therefore, one deduces straightforwardly from (5.16) the following Lemma.

Lemma 5.5.27. *([196]) Let $n = 2m$ with m odd. Let $a' \in \mathbb{F}_{2^n}^\star$ and $b' \in \mathbb{F}_4^\star$. Suppose that $a' = a\zeta^i v$ with $a \in \mathbb{F}_{2^m}^\star$ $i \in \{0,1,2\}$, ζ be a generator of the cyclic group $U := \{u \in \mathbb{F}_{2^n}^\star \mid u^{2^m+1} = 1\}$ and, $v \in V := \{u^3 \mid u \in U\}$. Then, there exists $b \in \mathbb{F}_4^\star$ such that $g_{a',b'}$ is linearly equivalent to $g_{a\zeta^i,b}$.*

Every element $a' \in \mathbb{F}_{2^n}^\star$ can be (uniquely) decomposed as $a' = a\zeta^i v$ with $a \in \mathbb{F}_{2^m}^\star$, $i \in \{0,1,2\}$, ζ be a generator of the cyclic group $U := \{u \in \mathbb{F}_{2^n}^\star \mid u^{2^m+1} = 1\}$ and, $v \in V := \{u^3 \mid u \in U\}$. Therefore, according to the preceding Lemma, *one can restrict oneself to study the bentness of $g_{a\zeta^i,b}$ with $a \in \mathbb{F}_{2^m}^\star$ $b \in \mathbb{F}_4^\star$.*

• Now collect the material that we have obtained to study the (hyper)-bentness of functions in $\mathfrak{G}_n$.

Lemma 5.5.28. *([196]) Let $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_4^\star$. Suppose that m is odd. Then, a function $g_{a,b}$ of the family $\mathfrak{G}_n$ is bent if and only if $\Gamma(a,b) := \sum_{u\in U} \chi(g_{a,b}(u)) = 1$. Moreover, bent functions $g_{a,b}$ of the family $\mathfrak{G}_n$ belong to the Partial Spreads class $\mathcal{PS}^-$.*

Proof. Recall that every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as: $x = yu$, with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U := \{u \in \mathbb{F}_{2^n}^\star \mid u^{2^m+1} = 1\}$. Then, since 3 divides $2^m + 1$ when m is odd, for every $x \in \mathbb{F}_{2^n}^\star$, we have

$$g_{a,b}(x) = g_{a,b}(uy) = \mathrm{Tr}_1^n\left(au^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bu^{\frac{2^n-1}{3}}\right) = g_{a,b}(u) \tag{5.18}$$

The function $g_{a,b}$ is then constant on the cosets $u\mathbb{F}_{2^m}^\star$, $u \in U$. Therefore, the support of $g_{a,b}$ can be decomposed into the disjoint union sets (with the null vector, these sets are vector subspaces of dimension 2^m) as follows

$$supp(g_{a,b}) = \bigcup_{u\in S_{a,b}} u\mathbb{F}_{2^m}^\star \text{ where } S_{a,b} := \{u \in U \mid g_{a,b}(u) = 1\}. \tag{5.19}$$

According to Theorem 4.4.2, this implies that the bentness of $g_{a,b}$ is equivalent to the fact that the Hamming weight of the restriction of $g_{a,b}$ to U is equal to 2^{m-1} and that bent functions $g_{a,b}$ of the class $\mathfrak{G}_n$ are in the class $\mathcal{PS}^-$. To conclude, it suffices to note that $\Gamma(a,b) = \#U - 2\,\mathrm{wt}(g_{a,b}|_U)$ ($\#U = 2^m + 1$). □

We have seen that, when m is odd, bent functions $g_{a,b}$, with $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_4^\star$ are in the class PS^- class. In the following, we will give a more precise statement of Lemma 5.5.28 , in particular, we will see that when m is odd then, bent Boolean functions of $\mathfrak{G}_n$ are in the class of hyper-bent Boolean functions.
Thus, according to Proposition 5.4.2, Proposition 5.4.4 and Lemma 5.5.28, one can straightforwardly deduce a more precise statement of Lemma 5.5.28.

Proposition 5.5.29. *([196]) Let $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_4^\star$. Let $g_{a,b}$ be a Boolean function belonging to the family $\mathfrak{G}_n$,($n = 2m$, m odd). Then $g_{a,b}$ is hyper-bent if and only if $\Gamma(a,b) := \sum_{u\in U} \chi(g_{a,b}(u)) = 1$ (where U denotes the set of the (2^m+1)-th roots of unity in $\mathbb{F}_{2^n}$). Moreover, $g_{a,b}$ is in the class $\mathcal{PS}_{ap}$ if and only if $\mathrm{Tr}_1^n(a) + \mathrm{Tr}_1^2(b) = 0$.*

Proof. If α is a primitive element of $\mathbb{F}_{2^n}$ then, $g_{a,b}(\alpha^{2^m+1}x) = g_{a,b}(x)$ for every $x \in \mathbb{F}_{2^n}$ (since 3 divides $2^m + 1$ when m is odd) and 0 is not in the support of $g_{a,b}$. The conditions of the bentness given by Proposition 5.4.2 are then satisfied thanks to Lemma 5.5.28. The second part of the Proposition is a direct application of Proposition 5.4.4. □

According to Lemma 8.1.10 and Proposition 5.5.29, the question of deciding whether an element $g_{a,b}$ of $\mathfrak{G}_n$ is hyper-bent or not can be reduced to computing the sum $\Gamma(a\zeta^i, \beta^j)$ for $(i,j) \in \{0,1,2\}^2$. For that, we shall use Proposition 2.3.6 in Section 2.3 (Chapter **??**).

Now, recall that $V := \{u^3 \mid u \in U\}$. Let ζ be a generator of the cyclic group U. We introduce the sums

$$\forall a \in \mathbb{F}_{2^m}^\star, \forall i \in \{0,1,2\}, \quad S_i(a) = \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^i v). \tag{5.20}$$

The sums $S_i(a)$ can be expressed in terms of Kloosterman sums and cubic sums. These expressions can be obtained from Proposition 9 in [195]. For completeness, we include the proof.

Lemma 5.5.30. *([196]) For every $a \in \mathbb{F}_{2^m}^\star$, we have:*

$$S_0(a) = \frac{1 - K_m(a) + 2C_m(a,a)}{3}, \quad S_2(a) = S_1(a) = \frac{1 - K_m(a) - C_m(a,a)}{3}$$

Proof. Note firstly that the mapping $x \mapsto x^3$ being 3-to-1 on U, then, thanks to Lemma 2.3.6, one has

$$\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av) = \frac{1}{3} \sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^3)) = \frac{1}{3}\big(1 - K_m(a) + 2C_m(a,a)\big)$$

Now, since ζ^{2^m-2} is an element of V (because 3 divides (2^m+1)) and the mapping $v \mapsto \zeta^{2^m-2}v^{2^m}$ is a permutation on V, then, we have:

$$\begin{aligned} S_1(a) &= \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta v)) = \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^{2^m} v^{2^m})) \\ &= \sum_{v \in V} \chi(\mathrm{Tr}_1^n(a\zeta^2(\zeta^{2^m-2} v^{2^m}))) = S_2(a) \end{aligned}$$

Next, using the fact that $\sum_{u \in G} \chi(\mathrm{Tr}_1^n(au)) = 1 - K_m(a)$, where G is a cyclic group of order $2^m + 1$, we obtain :

$$S_0(a) + S_1(a) + S_2(a) = \sum_{u \in U} \chi(\mathrm{Tr}_1^n(au)) = 1 - K_m(a)$$

Therefore, $S_1(a) = \frac{1 - K_m(a) - S_0(a)}{2}$. To conclude, it suffices to note that, the mapping $x \mapsto x^3$ being 3-to-1 from U to itself, one has $\sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^3)) = 3S_0(a)$ and that $\sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^3)) = 1 - K_m(a) + 2C_m(a,a)$ according to Lemma 2.3.6. □

• At this stage, we have the material to study of the (hyper)-bentness of Boolean functions belonging to the family $\mathfrak{G}_n$.

Proposition 5.5.31. *([196]) Let $n = 2m$ be an even integer with m odd. Let $a \in \mathbb{F}_{2^m}^\star$, β be a primitive element of $\mathbb{F}_4$ and ζ be a generator of the cyclic group U of (2^m+1)-th of unity. Suppose that $\mathrm{Tr}_1^m(a^{1/3}) = 0$. For $(i,j) \in \{0,1,2\}^2$, let $g_{a\zeta^i,\beta^j}$ be a Boolean function defined on $\mathbb{F}_{2^n}$ whose expression is of the form (5.15). Suppose that $m \not\equiv 3 \pmod 6$. Then, $g_{a\zeta^i,\beta^j}$ is bent if and only if $K_m(a) = 4$.*

Proof. Recall that, $\Gamma(a,b)$ denotes the sum $\sum_{u \in U} \chi(g_{a,b}(u))$.
For $(i,j) \in \{0,1,2\}^2$, we have (using the fact that the mapping $u \mapsto u^{2^m-1}$ is a permutation of U)

$$\Gamma(a\zeta^i,\beta^j) := \sum_{u\in U}\chi\left(g_{a\zeta^i,\beta^j}(u)\right) = \sum_{u\in U}\chi\left(\mathrm{Tr}_1^n(a\zeta^i u^{3(2^m-1)}) + \mathrm{Tr}_1^2(\beta^j u^{\frac{2^n-1}{3}})\right)$$
$$= \sum_{u\in U}\chi\left(\mathrm{Tr}_1^n(a\zeta^i u^3) + \mathrm{Tr}_1^2(\beta^j u^{\frac{2^m+1}{3}})\right)$$

Now, thanks to (5.17), we have seen that every element $u\in U$ can be uniquely decomposed as $u=\zeta^l v$ with $l\in\{0,1,2\}$ and $v\in V := \{u^3 \mid u\in U\}$. Hence, for $(i,j)\in\{0,1,2\}^2$, we have (in the last equality, we use the fact that v is a cube of an element of U which is a group of order 2^m+1)

$$\Gamma(a\zeta^i,\beta^j) = \sum_{l=0}^{2}\sum_{v\in V}\chi\left(\mathrm{Tr}_1^n(a\zeta^{3l+i}v^3) + \mathrm{Tr}_1^2(\beta^j\zeta^{l\frac{2^m+1}{3}}v^{\frac{2^m+1}{3}})\right)$$
$$= \sum_{l=0}^{2}\sum_{v\in V}\chi\left(\mathrm{Tr}_1^n(a\zeta^{3l+i}v^3) + \mathrm{Tr}_1^2(\beta^j\zeta^{l\frac{2^m+1}{3}})\right)$$

Next, $m\not\equiv 3 \pmod 6$ then, integers 3 and $\frac{2^m+1}{3}$ are co-prime. The mapping $x\mapsto x^3$ is then a permutation of V and thus for $(i,j)\in\{0,1,2\}^2$, we have (in the last equality, we use the fact that the mapping $v\mapsto\zeta^{3l}v$ is a permutation of V)

$$\begin{aligned}\Gamma(a\zeta^i,\beta^j) &= \sum_{l=0}^{2}\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\zeta^{3l+i}v) + \mathrm{Tr}_1^2(\beta^j\zeta^{l\frac{2^m+1}{3}}))\\ &= \sum_{l=0}^{2}\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\zeta^{i}v) + \mathrm{Tr}_1^2(\beta^j\zeta^{l\frac{2^m+1}{3}}))\end{aligned}$$

But, for every $j\in\{0,1,2\}$, the set $\{\beta^j,\beta^j\zeta^{\frac{2^m+1}{3}}\beta^j\zeta^{2\frac{2^m+1}{3}}\}$ is equal to $\mathbb{F}_4^\star$ (which contains two elements of absolute trace 1 on $\mathbb{F}_4$ and one element of absolute trace 0 on $\mathbb{F}_4$). We thus conclude that

$$\Gamma(a\zeta^i,\beta^j) = -\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\zeta^i v)) =: -S_i(a). \tag{5.21}$$

Next, since m is odd, the mapping $x\mapsto x^3$ is permutation on $\mathbb{F}_{2^m}$. Hence, every element $a\in\mathbb{F}_{2^m}$ can be (uniquely) written as $a=c^3$ with $c\in\mathbb{F}_{2^m}$. One has

$$C_m(a,a) := \sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(ax^3+ax)) = \sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m((cx)^3+ax))$$
$$= \sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m((cx)^3+a^{2/3}(cx))) = \sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^3+a^{2/3}x)) = C_m(1,a^{2/3}).$$

Now, since $\mathrm{Tr}_1^m(a^{2/3}) = \mathrm{Tr}_1^m(a^{1/3})$ and $\mathrm{Tr}_1^m(a^{1/3}) = 0$ (by hypothesis), one has $C_m(a,a)=0$, according to Proposition 2.2.5. Therefore, thanks to Lemma 5.5.30, we obtain

$$\Gamma(a\zeta^i,\beta^j) = \frac{K_m(a)-1}{3}.$$

We conclude thanks to Lemma 5.5.28. □

Proposition 5.5.32. *([196]) Let $n = 2m$ be an even integer with m odd. Let $a \in \mathbb{F}_{2^m}^\star$, β be a primitive element of $\mathbb{F}_4$ and, ζ be a generator of the cyclic group U of (2^m+1)-th of unity. Suppose that $\mathrm{Tr}_1^m(a^{1/3}) = 1$. For $(i,j) \in \{0,1,2\}^2$, let $g_{a\zeta^i,\beta^j}$ be a Boolean function on $\mathbb{F}_{2^n}$ whose expression is of the form (5.15). Assume that $m \not\equiv 3 \pmod 6$. Then*

1. *The function g_{a,β^j} is not bent for every $j \in \{0,1,2\}$.*
2. *For every $i \in \{1,2\}$ and $j \in \{0,1,2\}$, the function $g_{a\zeta^i,\beta^j}$ is bent if and only if $K_m(a) + C_m(a,a) = 4$.*

Proof. We have seen in the proof of Proposition 5.5.31, that $C_m(a,a) = C_m(1,a^{2/3})$. Then, according to Proposition 2.2.5, one has $C_m(a,a) = \epsilon_a \left(\frac{2}{m}\right) 2^{(m+1)/2}$ with $\epsilon_a = \pm 1$ (since $\mathrm{Tr}_1^m(a^{2/3}) = \mathrm{Tr}_1^m(a^{1/3})$ and $\mathrm{Tr}_1^m(a^{1/3}) = 1$, by hypothesis).

1. Let $j \in \{0,1,2\}$. According to (5.21), valid only if $m \not\equiv 3 \pmod 6$, and thanks to Lemma 5.5.30, we have that $\Gamma(a,\beta^j) = \frac{K_m(a)-1-\epsilon_a\left(\frac{2}{m}\right)2^{(m+3)/2}}{3}$. Then, according to Lemma 5.5.28, the Boolean function g_{a,β^j} is therefore bent if and only if $K_m(a) = 4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2}$, which is impossible for $m > 3$, since the Kloosterman sums $K_m(a)$ take values in the range $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$, according to Proposition 2.2.2.
2. According to (5.21) and Lemma 5.5.30, for every $i \in \{1,2\}$ and $j \in \{0,1,2\}$, we have $\Gamma(a\zeta^i,\beta^j) = \frac{K_m(a)+C_m(a,a)-1}{3}$. The Boolean function $g_{a\zeta^i,\beta^j}$ is therefore bent if and only if $K_m(a) + C_m(a,a) = 4$, according to Lemma 5.5.28.

□

Remark 5.5.33. *Since the cubic sums $C_m(a,a)$ equal $\epsilon_a \left(\frac{2}{m}\right) 2^{(m+1)/2}$ with $\epsilon_a = \pm 1$ (when $\mathrm{Tr}_1^m(a^{1/3}) = 1$, m odd) and the Jacobi symbol $\left(\frac{2}{m}\right)$ equals $(-1)^{\frac{(m^2-1)}{8}}$ (when m is odd) then, the condition $K_m(a) + C_m(a,a) = 4$ on $a \in \mathbb{F}_{2^m}^\star$ says that the Kloosterman sums $K_m(a)$ take the values $4 \pm 2^{(m+1)/2}$.*

Proposition 5.5.34. *([196]) Let $n = 2m$. Suppose that m is odd such that $m \equiv 3 \pmod 6$. Let $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4$ and, ζ be a generator of the cyclic group U of (2^m+1)-th of unity. For $i \in \{0,1,2\}$, let $g_{a\zeta^i,b}$ be a Boolean function on $\mathbb{F}_{2^n}$ whose expression is of the form (5.15). Then, $g_{a\zeta^i,b}$ is not bent.*

Proof. According to Lemma 8.1.10 and Lemma 5.5.28, it suffices to compute the value $\sum_{u\in U} \chi(g_{a\zeta^i,b}(u))$ to decide whether $g_{a\zeta^i,b}$ is bent or not. Note now that (recall that 9 divides 2^m+1 if $m \equiv 3 \pmod 6$)

$$\sum_{u\in U} \chi(g_{a\zeta^i,b}(u)) = \sum_{u\in U} \chi(\mathrm{Tr}_1^n(a\zeta^i u^{3(2^m-1)}) + \mathrm{Tr}_1^2(bu^{3(2^m-1)\cdot\frac{2^m+1}{9}}))$$

The mapping $x \mapsto x^{3(2^m-1)}$ is 3-to-1 from U to itself. Thus, we get that

$$\sum_{u\in U} \chi(g_{a\zeta^i,b}(u)) = 3\sum_{v\in V} \chi(\mathrm{Tr}_1^n(a\zeta^i v) + \mathrm{Tr}_1^2(bv^{\frac{2^m+1}{9}}))$$

where $V = \{u^3 \mid u \in U\}$. The sum $\sum_{u\in U} \chi(g_{a\zeta^i,b}(u))$ is therefore a multiple of 3 and cannot be equal to 1 implying that $g_{a\zeta^i,b}$ cannot be bent. □

Collecting the results obtained in Proposition 5.5.31, Proposition 5.5.32 and Proposition 5.5.34 we obtain the following characterization of the bentness for Boolean function of the form (5.15).

Theorem 5.5.35. *([196]) Let $n = 2m$. Suppose that m is odd. Let $a \in \mathbb{F}_{2^m}^\star$. Let β be a primitive element of $\mathbb{F}_4$. Let ζ be a generator of the cyclic group U of (2^m+1)-th of unity. For $(i,j) \in \{0,1,2\}^2$, let $g_{a\zeta^i,\beta^j}$ be a Boolean function on $\mathbb{F}_{2^n}$ whose expression is of the form (5.15).*

1. *Assume $m \not\equiv 3 \pmod 6$. Then, we have:*
   - *If $\mathrm{Tr}_1^m(a^{1/3}) = 0$ then, for every $(i,j) \in \{0,1,2\}^2$, a function $g_{a\zeta^i,\beta^j}$ is (hyper)-bent if and only if $K_m(a) = 4$.*
   - *If $\mathrm{Tr}_1^m(a^{1/3}) = 1$ then:*
     (a) g_{a,β^j} is not bent for every $j \in \{0,1,2\}$.
     (b) For every $i \in \{1,2\}$, $g_{a\zeta^i,\beta^j}$ is (hyper)-bent if and only if $K_m(a) + C_m(a,a) = 4$.
2. *Assume $m \equiv 3 \pmod 6$. Then, for every $i \in \{0,1,2\}$, $g_{a\zeta^i,b}$ is not bent for every $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$.*

Example 5.5.36. *Let us describe for example the set of bent Boolean functions $g_{a,b}$ belonging to the class $\mathfrak{G}_{10}$ (with $b \neq 0$), that is, of the form $\mathrm{Tr}_1^{10}(ax^{93}) + \mathrm{Tr}_1^2(bx^{341})$ where $a \in \mathbb{F}_{2^{10}}^\star$ and $b \in \mathbb{F}_4^\star$.*
Let α be a primitive element of $\mathbb{F}_{32} = \mathbb{F}_2(\alpha)$ with $\alpha^5 + \alpha^2 + 1 = 0$. Let ξ be a primitive element of $\mathbb{F}_{2^{10}}$. According to table 4 in [56], the set $\{a \in \mathbb{F}_{2^5}^\star, \mathrm{Tr}_1^5(a^{1/3}) = 0\}$ is equal to $\{\alpha^3, \alpha^{21}, \alpha^{14}\}$ and, the set $\{a \in \mathbb{F}_{2^5}^\star, \mathrm{Tr}_1^5(a^{1/3}) = 1\}$ is equal to $\{1, \alpha^2, \alpha^9, \alpha^{15}\}$. The elements a of $\mathbb{F}_{2^5}^\star$ whose the Kloosterman sums $K_5(a)$ on $\mathbb{F}_{2^5}$ equals 4 (those elements a satisfy necessary $\mathrm{Tr}_1^5(a^{1/3}) = 0$) are α^3 and α^{21} while, those such that $K_5(a) + C_5(a,a) = 4$ are 1 and α^9 (more precisely, we have $K_5(1) = 12$ and $K_5(\alpha^9) = -4$).
According to Theorem 5.5.35 and Lemma 8.1.10 we conclude that there exist 330 hyper-bent Boolean functions defined on the field $\mathbb{F}_{2^{10}}$ belonging to the class $\mathfrak{G}_{10}$ (with $b \neq 0$). Such functions are $g_{\alpha^3 v,b}$, $g_{\alpha^{21} v,b}$, $g_{\xi^{31} v,b}$, $g_{\alpha^3\xi^{31} v,b}$, $g_{\alpha^9\xi^{31} v,b}$, $g_{\alpha^{21}\xi^{31} v,b}$, $g_{\xi^{62} v,b}$, $g_{\alpha^3\xi^{62} v,b}$, $g_{\alpha^9\xi^{62} v,b}$, $g_{\alpha^{21}\xi^{62} v,b}$, with $b \in \mathbb{F}_4^\star$ and v runs through the set $\{u^3 \mid u \in U\}$ where U is the cyclic group of 33-rd root of unity of $\mathbb{F}_{2^{10}}$.

Example 5.5.37. *Let $n = 14$ then, according to table 4 in [56], we find that there exist 1935 hyper-bent Boolean functions $g_{a,b}$ (with $b \neq 0$) defined on the field $\mathbb{F}_{16384}$ belonging to the class $\mathfrak{G}_{14}$. Such functions are of the form*

- $\mathrm{Tr}_1^{14}(cvx^{381}) + \mathrm{Tr}_1^2(bx^{5461})$, $c \in \{\alpha^{14}, \alpha^{15}, \alpha^{62}\}$,
- $\mathrm{Tr}_1^{14}(c'\xi^{127i}vx^{381}) + \mathrm{Tr}_1^2(bx^{5461})$, $i \in \{1,2\}$, $c' \in \{1, \alpha^{14}, \alpha^{15}, \alpha^{21}, \alpha^{62}, \alpha^{93}\}$,

where α is a primitive element of $\mathbb{F}_{128}$ satisfying $\alpha^7 + \alpha^3 + 1 = 0$, ξ is a primitive element of $\mathbb{F}_{2^{14}}$, v runs through the set $\{u^3 \mid u \in U\}$ where U is the cyclic group of 129-th root of unity of $\mathbb{F}_{2^{14}}$ and $b \in \{1, \beta, \beta^2\}$ where β is a primitive element of $\mathbb{F}_4$.

Example 5.5.38. *Let $n = 18$ then, according to Theorem 5.5.35, there exist no bent Boolean functions in the class $\mathfrak{G}_{18}$.*

Now, the dual functions of elements of $\mathfrak{G}_n$ can be explicitly computed as follows.

Proposition 5.5.39. *([196]) Let $n = 2m$ with m odd. Let $(a,b) \in \mathbb{F}_{2^n}^\star \times \mathbb{F}_4^\star$. The dual function of a bent function $g_{a,b}$ of $\mathfrak{G}_n$ is equal $g_{a^{2^m},b^2}$, that is, we have*

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{g_{a,b}}}(\omega) = 2^m \chi(g_{a^{2^m},b^2}(\omega)).$$

Proof. The arguments are for the most part the same as those used in [197]. Nevertheless, for the sake of completeness, we present below a little shorter proof. Recall that, since the function $g_{a,b}$ is assumed to be bent then, according to Lemma 5.5.28, $\sum_{u\in U}\chi(g_{a,b}(u))=1$. Given, $\omega\in\mathbb{F}_{2^n}$, since every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as : $x=yu$, with $y\in\mathbb{F}_{2^m}^\star$ and $u\in U$, one has (in the last equality, we use (5.18))

$$\begin{aligned}\widehat{\chi_{g_{a,b}}}(w) &:= \sum_{x\in\mathbb{F}_{2^n}}\chi(g_{a,b}(x)+\mathrm{Tr}_1^n(wx))\\ &= 1+\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star}\chi(g_{a,b}(yu)+\mathrm{Tr}_1^n(wyu))\\ &= 1+\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star}\chi(g_{a,b}(u)+\mathrm{Tr}_1^n(wyu))\end{aligned}$$

Note first that $\widehat{\chi_{g_{a,b}}}(0)=2^m$. Now, if w is an element of $\mathbb{F}_{2^n}^\star$, we have $\mathrm{Tr}_m^n(wu)=0$ if and only if $uw+u^{2^m}w^{2^m}=0$, that is, $u^{2^m-1}=w^{1-2^m}$. Classical results about character sums says that

$$\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^n(\omega uy))=\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\omega u)y))=2^m$$

if $\mathrm{Tr}_m^n(\omega u)=0$, that is, if $u^{2^m-1}=\omega^{1-2^m}$ and, is equal to 0 otherwise. Hence, using properties of trace functions, we have

$$\begin{aligned}\widehat{\chi_{g_{a,b}}}(w) &= 1+\sum_{u\in U}\chi(g_{a,b}(u))\left(\sum_{y\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^n(wyu))-1\right)\\ &= 1-\sum_{u\in U}\chi(g_{a,b}(u))+2^m\sum_{\substack{u\in U\\ \mathrm{Tr}_m^n(wu)=0}}\chi(g_{a,b}(u))\\ &= 2^m\chi(\mathrm{Tr}_1^n(aw^{3(1-2^m)})+\mathrm{Tr}_1^2(bw^{\frac{1-2^n}{3}}))\\ &= 2^m\chi(\mathrm{Tr}_1^n(a^{2^m}w^{3(2^m-1)})+\mathrm{Tr}_1^2(b^{2^m}w^{\frac{2^n-1}{3}}))\\ &= 2^m\chi(\mathrm{Tr}_1^n(a^{2^m}w^{3(2^m-1)})+\mathrm{Tr}_1^2(b^2w^{\frac{2^n-1}{3}}))=2^m\chi(g_{a^{2^m},b^2}(\omega))\end{aligned}$$

($b^{2^m-2}=1$ because m is being odd then, 3 divides (2^m+1) and then divides (2^m-2)). □

Now, recall that a bent function defined on $\mathbb{F}_{2^n}$ is said to be normal if it is constant on an $\frac{n}{2}$-dimensional flat $b+E$ where E is a subspace of $\mathbb{F}_{2^{\frac{n}{2}}}$.

Proposition 5.5.40. *([196]) The bent functions $g_{a,b}$ of $\mathfrak{G}_n$ (where $n=2m$ with m odd) are normal.*

Proof. Recall that $g_{a,b}$ is constant on each set $u\mathbb{F}_{2^m}^\star$, $u\in U=\{x\in\mathbb{F}_{2^n}^\star \mid x^{2^m+1}=1\}$. Choose then u such that $g_{a,b}(u)=0$. Then $g_{a,b}$ is constant of the vector space $u\mathbb{F}_{2^m}$ (of dimension m) proving that $g_{a,b}$ is normal. □

Remark 5.5.41. *By computer experiments, for small values of n ($n\leq 14$, because of the complexity of the problem) we have found that, the family $\mathfrak{G}_n$ does not contain bent functions when $m=\frac{n}{2}$ is even.*

The following theorem summarizes the results presented above related to the bentness of the functions $g_{a,b}$ of the family $\mathfrak{G}_n$.

Theorem 5.5.42. *([196]) Let $n = 2m$ with m odd. Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$. Let β be a primitive element of $\mathbb{F}_4$ and ζ be a generator of the cyclic group U of (2^m+1)-th of unity. Let $g_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by (5.15).*

1. *The algebraic degree of $g_{a,b}$ equals m (bent functions $g_{a,b}$ are then of maximal algebraic degree).*
2. *$g_{a,b}$ is hyper-bent if and only if $g_{a,b}$ is bent.*
3. *If $g_{a,b}$ is bent then its dual function equals $g_{a^{2^m},b^2}$.*
4. *The bent functions $g_{a,b}$ are in the class $\mathcal{PS}^-$. Moreover, the bent functions $g_{a,b}$ are elements of the Partial Spread class $\mathcal{PS}_{ap}$ (resp. $\mathcal{PS}_{ap}^\#$) if $b = 1$ (resp. if $b \neq 1$).*

Moreover,
**) Assume $m \not\equiv 3 \pmod 6$.*
-If $\mathrm{Tr}_1^m(a^{1/3}) = 0$ then, for every $(i,j) \in \{0,1,2\}^2$, $g_{a\zeta^i,\beta^j}$ is bent if and only if $K_m(a) = 4$.
-If $\mathrm{Tr}_1^m(a^{1/3}) = 1$ then
a) g_{a,β^j} is not bent for every $j \in \{0,1,2\}$.
b) for every $i \in \{1,2\}$, $j \in \{0,1,2\}$, $g_{a\zeta^i,\beta^j}$ is bent if and only if $K_m(a) + C_m(a,a) = 4$.
***) Assume $m \equiv 3 \pmod 6$. Then, for every $i \in \{0,1,2\}$, $g_{a\zeta^i,b}$ is not bent.*

The third family of binomial hyper-bent functions

Adopting our approach [197], [196] (developed in the previous sections) Wang et al. studied in late 2011 the hyper-bentess of the following binomial family [257, 256] with an additional trace term on $\mathbb{F}_{16}$:

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$$

where the coefficients a are in $\mathbb{F}_{2^m}$ $(m = \frac{n}{2})$, the coefficient b is in $\mathbb{F}_{16}$ and m must verify $m \equiv 2 \pmod 4$. They characterize the hyper-bentness where $r \equiv 0 \pmod 5$ and in the case where $r \not\equiv 0 \pmod 5$ and $(b+1)(b^4+b+1) = 0$ in terms of Kloosterman sums and using the factorization of $x^5 + x + a^{-1}$. We summarize their result in the following theorem

Theorem 5.5.43. *([257, 256]) Let $n = 2m$ and $m = 2m_1$ with $m_1 \equiv 2 \pmod 4$. and $m_1 \geq 3$. Let $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{16}^\star$. Let $f_{a,b}^{(r)}$ be the function defined on $\mathbb{F}_{2^n}$ by*

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$$

1. *If $b = 1$ then $f_{a,1}$ is hyper-bent iff $p(X) = X^5 + X + a^{-1}$ is irreducible over $\mathbb{F}_{2^m}$ and the quadratic form $q(x) = \mathrm{Tr}_1^m(x(ax^4 + ax^2 + a^2x))$ over $\mathbb{F}_{2^m}$ is even and $K_m(a) = \frac{4}{3}(2 - 2^{m_1})$.*
2. *if b is a primitive element of $\mathbb{F}_{16}^\star$ such that $\mathrm{Tr}_1^4(b) = 0$ then $f_{a,b}$ is hyper-bent iff $p(X) = X^5 + X + a^{-1}$ is irreducible over $\mathbb{F}_{2^m}$, the quadratic form $q(x) = \mathrm{Tr}_1^m(x(ax^4 + ax^2 + a^2x))$ over $\mathbb{F}_{2^m}$ is even and $K_m(a) = 2 \cdot 2^{m_1} - 4$.*

Moreover, they give all the hyper-bent functions in the case where $a \in \mathbb{F}_{2^{\frac{m}{2}}}$. The reader can refer to the following references of the authors [257, 256].

Chapter 6

Hyper-bent functions with multiple trace terms via Dillon-like exponents

Contents

6.1 Hyper-bent functions with multiple trace terms via Dillon (like) expnents: the Charpin and Gong family

Let E' be a set of representatives of the cyclotomic cosets modulo 2^m+1 for which each coset has the maximal size n. Let f_{a_r} be the function defined on $\mathbb{F}_{2^n}$ by

$$f_{a_r}(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) \tag{6.1}$$

where $a_r\in\mathbb{F}_{2^n}$ and $R\subseteq E'$. Charpin and Gong [54] have studied the bentness of the class of Boolean functions f_{a_r} defined on $\mathbb{F}_{2^n}$ by (6.1) and denoted by $\mathcal{F}_n$ in the case when all the coefficients a_r are in $\mathbb{F}_{2^m}$.

They introduced a new tool by means of Dickson polynomials to describe hyper-bent functions f_{a_r}. In particular, when r is co-prime with 2^m+1, the functions f_{a_r} are the sum of several Dillon monomial functions; the link between the Dillon monomial hyper-bent functions and the zeros of some Kloosterman sums has been generalized to a link between hyper-bent functions f_{a_r} of this class and some exponential sums where Dickson polynomials are involved. More precisely, Charpin and Gong have proved the following result.

Theorem 6.1.1. *([54]) Let f_{a_r} be the function defined on $\mathbb{F}_{2^n}$ by (6.1) where $a_r\in\mathbb{F}_{2^m}$. Let g_{a_r} be the related Boolean function defined on $\mathbb{F}_{2^m}$ by $g_{a_r}(x)=\sum_{r\in R}\mathrm{Tr}_1^m(a_rD_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then f_{a_r} is hyper-bent if and only if $\sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^{-1})+g_{a_r}(x))=2^m-2\,\mathrm{wt}(g_{a_r})$.*

By Theorem 6.1.1, Charpin and Gong have characterized the class of binomial hyperbent functions whose expression is of the form $\mathrm{Tr}_1^n\left(a\left(x^{(2^r-1)(2^m-1)}+x^{(2^r+1)(2^m-1)}\right)\right)$, where $a\in\mathbb{F}_{2^m}^\star$ and r is an integer such that $0<r<m$ and $\{2^r-1,2^r+1\}\subset E'$ (note that the functions of type (5.10) do not belong to this class). Continuing their interesting approach, Gologlu [114] has identified some trace representation of some hyper-bent functions and proved that the following functions defined on $\mathbb{F}_{2^n}$, are hyper-bent:

- $x\mapsto\sum_{i=1}^{2^{m-1}-1}\mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$, $\beta\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2$.
- $x\mapsto\sum_{i=1}^{2^{m-2}-1}\mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$ where, m odd and $\beta^{(2^m-4)^{-1}}\in\{x\in\mathbb{F}_{2^m}^*\mid\mathrm{Tr}_1^m(x)=0\}$.

6.2 Hyper-bent functions with multiple trace terms via Dillon (like) expnents: the family $\mathfrak{H}_n$

In the sequel, n is an even positive integer, $m=\frac{n}{2}$ is an odd integer and E is a set of representatives of the cyclotomic classes modulo 2^n-1 for which each class has the full size n. We denote by $\mathfrak{H}_n$ the set of Boolean functions $f_{a_r,b}$ defined on $\mathbb{F}_{2^n}$ whose polynomial forms are:

$$f_{a_r,b}(x):=\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{r(2^m-1)})+\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}). \tag{6.2}$$

where $R\subseteq E$, all the coefficients a_r are in $\mathbb{F}_{2^m}$ and $b\in\mathbb{F}_4^\star$.
Recall that the size of the cyclotomic coset of 2 modulo 2^n-1 containing $\frac{2^n-1}{3}$ is equal to 2 (i.e. $o(\frac{2^n-1}{3})=2$) and that, the function $f_{a_r,b}$ does not belong to the class considered by Charpin and Gong ([54]) in Subsection 6.1.

In the following, we show that hyper-bent functions of $\mathfrak{H}_n$ can be described by means of exponential sums involving Dickson polynomials (Theorem 6.2.10 and Theorem 6.2.8). In particular, when b is a primitive element of $\mathbb{F}_4$, we provide a way to transfer the characterization of hyper-bentness of an element of $\mathfrak{H}_n$ to the evaluation of the Hamming weight of some Boolean functions. To illustrate our results, we show that the results presented in the binomial case ([197], [196]) can be deduced. Finally, in the end of the subsection we provide a possibly new infinite family of hyper-bent functions provided that some sets are not empty (Conjecture 6.2.15 and Conjecture 6.2.17).

Study of the bentness of the family with multiple trace terms $\mathfrak{H}_n$

For m odd, 2^m+1 is a multiple of 3 and thus all exponents for x in (6.2) are multiples of 2^m-1. Therefore, every Boolean function $f_{a_r,b}$ in $\mathfrak{H}_n$ satisfies

$$\forall x \in \mathbb{F}_{2^n}, \quad f_{a_r,b}(\alpha^{2^m+1}x) = f_{a_r,b}(x).$$

where α denotes any primitive element of $\mathbb{F}_{2^n}$. Furthermore, since every Boolean $f_{a_r,b}$ of $\mathfrak{H}_n$ vanishes at 0, one can then apply Proposition 5.4.2 to get the following characterization of hyper-bentness for an element of $\mathfrak{H}_n$.

Proposition 6.2.1. *Let $f_{a_r,b} \in \mathfrak{F}_n$. Set $\Lambda(f_{a_r,b}) := \sum_{u\in U} \chi(f_{a_r,b}(u))$ where U is the group of (2^m+1)-st roots of unity, that is, $U = \{x \in \mathbb{F}_{2^n} \mid x^{2^m+1} = 1\}$. Then, $f_{a_r,b}$ is hyper-bent if and only if $\Lambda(f_{a_r,b}) = 1$. Moreover, a hyper-bent function $f_{a_r,b}$ is in the Partial Spreads class PS_{ap} if and only if $b \in \mathbb{F}_2$.*

Proof. The Boolean function $f_{a_r,b}$ satisfies the assumptions of Proposition 5.4.2. Therefore $f_{a_r,b}$ is hyper-bent if and only if its restriction to U has Hamming weight 2^{m-1} according to Proposition 5.4.2. Now, one has $\Lambda(f_{a_r,b}) = 2^m + 1 - 2|\{u \in U \mid f_{a_r,b}(u) = 1\}|$. Therefore, the Hamming weight of the restriction of $f_{a_r,b}$ to U equals 2^{m-1} if and only if $\Lambda(f_{a_r,b}) = 1$. The second part of the proposition is a direct application of Proposition 5.4.4. Indeed, note that $f_{a_r,b}(1) = \sum_{r\in R} \mathrm{Tr}_1^n(a_r) + \mathrm{Tr}_1^2(b) = \mathrm{Tr}_1^2(b)$ (since $\mathrm{Tr}_1^n(a_r) = 0$ for every $r \in R$ because $a_r \in \mathbb{F}_{2^m}$) and it is clear that the elements b of $\mathbb{F}_4$ whose trace over $\mathbb{F}_4$ equals 0, are the elements of $\mathbb{F}_2$. □

We are interested in characterizing the hyper-bentness of the Boolean function of the form (6.2). To this end, we begin by introducing some additional notation while underlining some facts.

Let β be a primitive element of $\mathbb{F}_4$. Suppose that $\beta = \alpha^{\frac{2^n-1}{3}}$ for some primitive element α of $\mathbb{F}_{2^n}$. Set $\xi := \alpha^{2^m-1}$ so that ξ is a generator of the cyclic group $U := \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$. Note that U can be decomposed as : $U = \bigcup_{i=0}^{2} \xi^i V$ where $V := \{u^3,\, u \in U\}$. Next, let introduce the sums

$$S_i := \sum_{v\in V} \chi(f_{a_r,0}(\xi^i v)), \quad \forall i \in \{0,1,2\} \tag{6.3}$$

First of all, note that

$$S_0 + S_1 + S_2 = \sum_{u\in U} \chi(f_{a_r,0}(u)). \tag{6.4}$$

Next, one has

Lemma 6.2.2. *([192]) $S_1 = S_2$.*

Proof. Since the trace map is invariant under the Frobenius automorphism $x \mapsto x^2$, we get applying m times the Frobenius automorphism : $\forall x \in \mathbb{F}_{2^n}$,

$$f_{a_r,0}(x) = \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r^{2^m} x^{2^m r(2^m-1)}\right) = \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r x^{2^m r(2^m-1)}\right) = f_{a_r,0}(x^{2^m})$$

because all the coefficients a_r are in $\mathbb{F}_{2^m}$. Hence,

$$S_1 = \sum_{v\in V} \chi(f_{a_r,0}(\xi^{2^m} v^{2^m})) = \sum_{v\in V} \chi(f_0(\xi^2(\xi^{2^m-2} v^{2^m}))).$$

Now, since m is odd, 3 divides 2^m+1 and then divides 2^m-2. Hence, ξ^{2^m-2} is a cube of U and the mapping $v \mapsto \xi^{(2^m-2)} v^{2^m}$ is a permutation of V. Consequently, $S_1 = \sum_{v\in V} \chi(f_0(\xi^2 v)) = S_2$. □

Now, for $b \in \mathbb{F}_4^\star$, we establish expressions for $\Lambda(f_{a_r,b}) := \sum_{u\in U} \chi(f_{a_r,b}(u))$ (where U is the group of (2^m+1)-st roots of unity) involving the sums S_i.

Proposition 6.2.3. *([192])* $\Lambda(f_{a_r,\beta}) = \Lambda(f_{a_r,\beta^2}) = -S_0$ *and* $\Lambda(f_{a_r,1}) = S_0 - 2S_1$.

Proof. Introduce for every element c of $\mathbb{F}_4$ $T(c) := \sum_{b\in\mathbb{F}_4} \Lambda(f_{a_r,b})\chi(\mathrm{Tr}_1^2(bc))$. Recall that one has

$$\Lambda(f_b) = \frac{1}{4} \sum_{c\in\mathbb{F}_4} T(c)\chi(\mathrm{Tr}_1^2(bc)). \tag{6.5}$$

Indeed

$$\begin{aligned}
&\sum_{c\in\mathbb{F}_4} T(c)\chi(\mathrm{Tr}_1^2(bc)) \\
&= \sum_{c\in\mathbb{F}_4} \sum_{d\in\mathbb{F}_4} \Lambda(f_d)\chi(\mathrm{Tr}_1^2(dc))\chi(\mathrm{Tr}_1^2(bc)) \\
&= \sum_{d\in\mathbb{F}_4} \Lambda(f_d) \sum_{c\in\mathbb{F}_4} \chi(\mathrm{Tr}_1^2(c(d+b)))
\end{aligned}$$

But $\sum_{c\in\mathbb{F}_4} \chi(\mathrm{Tr}_1^2(c(d+b))) = 4$ if $d = b$ (i.e $b+d=0$) and 0 otherwise. Then, one gets

$$\sum_{c\in\mathbb{F}_4} T(c)\chi(\mathrm{Tr}_1^2(bc)) = 4\Lambda(f_b).$$

Now, note that $T(c) = \sum_{u\in U} \chi(f_0(u)) \sum_{b\in\mathbb{F}_4} \chi\Big(\mathrm{Tr}_1^2\left(b\big(c+u^{\frac{2^n-1}{3}}\big)\right)\Big)$. Furthermore, one has

$$\sum_{b\in\mathbb{F}_4} \chi\Big(\mathrm{Tr}_1^2\left(b\big(c+u^{\frac{2^n-1}{3}}\big)\right)\Big) = 0 \text{ if } u^{\frac{2^n-1}{3}} \neq c \text{ and } 4 \text{ otherwise.}$$

Since, $u^{\frac{2^n-1}{3}} \neq 0$ for every $u \in U$, $T(0) = 0$. Since β is a primitive element of $\mathbb{F}_4$, let suppose from now that $c = \beta^i$, $i \in \{0,1,2\}$. Recall that $\beta = \alpha^{\frac{2^n-1}{3}}$ and $\xi = \alpha^{2^m-1}$ for some primitive element α of $\mathbb{F}_{2^n}$. Then $\beta^i = \xi^{i\frac{2^m+1}{3}}$. Hence, $T(\beta^i) = 4\sum_{u\in U,\, u^{\frac{2^n-1}{3}} = \beta^i = \xi^{i\frac{2^m+1}{3}}} \chi(f_0(u))$. Now,

$$u^{\frac{2^n-1}{3}} = \xi^{i\frac{2^m+1}{3}} \iff \left(u^{-2}\xi^{-i}\right)^{\frac{2^m+1}{3}} = 1 \iff u^{-2} \in \xi^i V.$$

That follows from the fact that the only elements x of U such that $x^{\frac{2^m+1}{3}} = 1$ are the elements of V. Next, noting that the map $x \mapsto x^{2^{m-1}}$ is one-to-one from $\xi^i V$ to $\xi^i V$ (because $\xi^{i(2^{m-1}-1)}$ is a cube since $2^{m-1} - 1 \equiv 0 \pmod 3$ for m odd), one gets that $u^{\frac{2^n-1}{3}} = \xi^{i\frac{2^m+1}{3}} \iff u \in \xi^i V$.

Therefore

$$T(\beta^i) = 4 \sum_{v \in V} \chi(f_0(\xi^i v)) = 4S_i.$$

Finally, by the inversion formula (8.9), one gets $\Lambda(f_{a_r,b}) = \frac{1}{4} \sum_{c \in \mathbb{F}_4} T(c)\chi(\mathrm{Tr}_1^2(bc))$ that is,

$$\begin{aligned}
\Lambda(f_{a_r,1}) &= S_0\chi(\mathrm{Tr}_1^2(1)) + S_1\chi(\mathrm{Tr}_1^2(\beta)) + S_2\chi(\mathrm{Tr}_1^2(\beta^2)),\\
\Lambda(f_{\beta}) &= S_0\chi(\mathrm{Tr}_1^2(\beta)) + S_1\chi(\mathrm{Tr}_1^2(\beta^2)) + S_2\chi(\mathrm{Tr}_1^2(1)),\\
\Lambda(f_{a_r,\beta^2}) &= S_0\chi(\mathrm{Tr}_1^2(\beta^2)) + S_1\chi(\mathrm{Tr}_1^2(1)) + S_2\chi(\mathrm{Tr}_1^2(\beta)).
\end{aligned}$$

The result follows then from Lemma 6.2.2 and from the fact that $\mathrm{Tr}_1^2(1) = 0$ and $\mathrm{Tr}_1^2(\beta) = \mathrm{Tr}_1^2(\beta^2) = 1$. □

From Proposition 6.2.1, Proposition 6.2.3, Lemma 6.2.2 and (6.4), one straight-forwardly deduces the following statement.

Lemma 6.2.4. *([192]) Let $n = 2m$ be an even integer with m odd. For $b \in \mathbb{F}_4$, let $f_{a_r,b}$ be a function defined by (6.2). Let β be a primitive element of $\mathbb{F}_4$. Let U be the cyclic group of (2^m+1)-st roots of unity and V be the set of the cube of U. Then,*

1. *$f_{a_r,\beta}$ is hyper-bent if and only if $\sum_{v \in V} \chi(f_0(v)) = -1$.*
2. *$f_{a_r,\beta}$ is hyper-bent if and only if f_{a_r,β^2} is hyper-bent.*
3. *$f_{a_r,1}$ is hyperbent if and only if $2\sum_{v \in V} \chi(f_{a_r,0}(v)) - \sum_{u \in U} \chi(f_{a_r,0}(u)) = 1$.*

Now we shall separate the case where $b = 1$ and the case where b is a primitive element of $\mathbb{F}_4$.

• The case where b is a primitive element of $\mathbb{F}_4$

According to Assertion (b) of Lemma 6.2.4, we can suppose that $b = \beta$ without loss of generality. As in the case where $b = 0$ (Theorem 6.1.1), one can establish a characterization of the hyper-bentness of f_β involving the Dickson polynomials. To this end, we begin with proving the following important technical result.

Lemma 6.2.5. *([192]) Let f_0 be the function defined on $\mathbb{F}_{2^n}$ by $f_0(x) := \sum_{r \in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$. Let g be the related function defined on $\mathbb{F}_{2^m}$ by $g(x) = \sum_{r \in R} \mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Let U be the cyclic group of (2^m+1)-st roots of unity. Then, for any positive integer p, we have*

$$\sum_{u \in U} \chi\Big(f_0(u^p)\Big) = 1 + 2 \sum_{c \in \mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(c^{-1})=1} \chi\Big(g(D_p(c))\Big).$$

Proof. Using the transitivity rule $\mathrm{Tr}_1^n = \mathrm{Tr}_1^m \circ \mathrm{Tr}_m^n$, the fact that the coefficients a_r are in the subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$ and the fact that the mapping $u \mapsto u^{2^m-1}$ is a permutation of U, one has

$$\begin{aligned}
&\sum_{u \in U} \chi\Big(f_0(u^p)\Big) = \sum_{u \in U} \chi\Big(\sum_{r \in R} \mathrm{Tr}_1^m\left(a_r(u^{(2^m-1)rp} + u^{2^m(2^m-1)rp})\right)\Big)\\
&= \sum_{u \in U} \chi\Big(\sum_{r \in R} \mathrm{Tr}_1^m\left(a_r(u^{rp} + u^{-rp})\right)\Big) = \sum_{u \in U} \chi\Big(\sum_{r \in R} \mathrm{Tr}_1^m\left(a_r D_{rp}(u + u^{-1})\right)\Big)
\end{aligned}$$

since $u^p + u^{-p} = D_p(u + u^{-1})$. Recall now that every element $1/c$ where $c \in \mathbb{F}_{2^m}^\star$ with $\mathrm{Tr}_1^m(c) = 1$ can be uniquely represented as $u + u^{2^m} = u + u^{-1}$ with $u \in U$. Thus

$$\begin{aligned}\sum_{u\in U} \chi\Big(f_0(u^p)\Big) &= 1 + \sum_{u\in U\setminus\{1\}} \chi\Big(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_{rp}(u+u^{-1})\right)\Big)\\ &= 1 + 2\sum_{c\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(c)=1} \chi\Big(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_{rp}(1/c)\right)\Big)\\ &= 1 + 2\sum_{c\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(c^{-1})=1} \chi\Big(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_{rp}(c)\right)\Big).\end{aligned}$$

In the last equality, we use the fact that the map $c \mapsto 1/c$ is a permutation on $\mathbb{F}_{2^m}$. Now, since $D_{rp} = D_r \circ D_p$, one gets

$$\sum_{u\in U} \chi\Big(f_0(u^p)\Big) = 1 + 2\sum_{c\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(c^{-1})=1} \chi\Big(g(D_p(c))\Big).$$

□

From Lemma 6.2.4 and Lemma 6.2.5, one deduce the following statement.

Theorem 6.2.6. *([192]) Let $n = 2m$ be an even integer with m odd. Let β be a primitive element of $\mathbb{F}_4$. Let $f_{a_r,\beta}$ be the function defined on $\mathbb{F}_{2^n}$ by (6.2). Let g be the related function defined on $\mathbb{F}_{2^m}$ by $g(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then, the three assertions are equivalent*

1. *$f_{a_r,\beta}$ is hyper-bent.*
2. $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big) = -2.$
3. $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + g(D_3(x))\Big) = 2^m - 2\,\mathrm{wt}(g\circ D_3) + 4.$

Proof. According to Lemma 6.2.5, we have

$$S_0 = \sum_{v\in V} \chi\Big(f_0(v)\Big) = \frac{1}{3}\sum_{u\in U} \chi\Big(f_0(u^3)\Big) = \frac{1}{3}\left(1 + 2\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big)\right).$$

The equivalence between assertions (a) and (b) in Theorem 6.2.10 follows then from assertion (1) of Lemma 6.2.4.

Now, note that the indicator of the set $\{x \in \mathbb{F}_{2^m}^\star \mid \mathrm{Tr}_1^m(x^{-1}) = 1\}$ can be written as $\frac{1}{2}\left(1 - \chi(\mathrm{Tr}_1^m(x^{-1}))\right)$. Therefore,

$$\begin{aligned}&\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big)\\ &\quad= \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}^\star} \chi\Big(g(D_3(x))\Big) - \sum_{x\in\mathbb{F}_{2^m}^\star} \chi\Big(\mathrm{Tr}_1^m(x^{-1} + g(D_3(x)))\Big)\right)\\ &\quad= \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(g(D_3(x))\Big) - \sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1} + g(D_3(x)))\Big)\right).\end{aligned}$$

Now, $f_{a_r,\beta}$ is hyper-bent if and only if $\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g(D_3(x))\Big)=-2$. Therefore, using the fact that, for a Boolean function h defined on $\mathbb{F}_{2^n}$, $\sum_{x\in\mathbb{F}_{2^n}}\chi(h(x))=2^n-2\,\mathrm{wt}(h)$, we get that f_β is hyper-bent if and only if

$$\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+g(D_3(x))\Big)=4+2^m-2\,\mathrm{wt}(g\circ D_3).$$

□

One also has

Proposition 6.2.7. *([192]) Let $n=2m$ be an even integer with m odd. Let d be a positive integer. Suppose that d and $\frac{2^m+1}{3}$ are co-prime. Let β be a primitive element of $\mathbb{F}_4$. Let $f_{a_r,\beta}$ be the function defined by (6.2) and $h_{a_r,\beta}$ be the function whose expression is*

$$\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{dr(2^m-1)})+\mathrm{Tr}_1^2(\beta x^{\frac{2^n-1}{3}})$$

where $a_r\in\mathbb{F}_{2^m}$. Then, $f_{a_r,\beta}$ is hyper-bent if and only if $h_{a_r,\beta}$ is hyper-bent.

Proof. According to assertion (a) of Lemma 6.2.4, $h_{a_r,\beta}$ is hyper-bent if and only if $\sum_{v\in V}\chi(h_0(v))=-1$. Now, $\sum_{v\in V}\chi(h_0(v))=\sum_{v\in V}\chi(f_0(v^d))=\sum_{v\in V}\chi(f_0(v))$ since the mapping $v\mapsto v^d$ is then a permutation of V if $\frac{2^m+1}{3}$ and d are co-prime. The result follows again from assertion (a) of Lemma 6.2.4. □

• The case where $b=1$:
we are interested in characterizing the hyper-bentness of the Boolean function $f_{a_r,1}$ whose polynomial form is $f_{a_r,1}(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{r(2^m-1)})+\mathrm{Tr}_1^2(x^{\frac{2^n-1}{3}})$. In this case one can give a characterization of the bentness, analogous to the assertion (b) of Theorem 6.2.10.

Theorem 6.2.8. *([192]) Let $n=2m$ be an even integer with m odd. Let $f_{a_r,1}$ be the Boolean function defined on $\mathbb{F}_{2^n}$ by*

$$f_{a_r,1}(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{r(2^m-1)})+\mathrm{Tr}_1^2(x^{\frac{2^n-1}{3}}).$$

Let g be the related function defined on $\mathbb{F}_{2^m}$ by $g(x)=\sum_{r\in R}\mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r.
Then, f_1 is hyper-bent if and only if,

$$2\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g(D_3(x))\Big)-3\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g(x)\Big)=2.$$

Proof. Note that

$$\begin{aligned}2\sum_{v\in V}\chi(f_0(v))-\sum_{u\in U}\chi(f_0(u))&=\frac{2}{3}\sum_{u\in U}\chi(f_0(u^3))-\sum_{u\in U}\chi(f_0(u))\\&=-\frac{1}{3}+\frac{4}{3}\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g(D_3(x))\Big)-2\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g(x)\Big)\end{aligned}$$

according to Lemma 8.1.16. One then concludes using Lemma 6.2.4 that states that f_1 is hyper-bent if and only if

$$2\sum_{v\in V}\chi(f_0(v))-\sum_{u\in U}\chi(f_0(u))=1.$$

□

One can also prove the similar result to Proposition 6.2.7.

Proposition 6.2.9. *([192]) Let $n=2m$ be an even integer with m odd. Suppose that $m\not\equiv 3 \pmod 6$. Let d be a positive integer such that $\gcd(d,2^m+1)=3$. Let β be a primitive element of $\mathbb{F}_4$. Let $f_{a_r,\beta}$ be the function defined by (6.2) and $h_{a_r,1}$ be the function whose expression is*

$$\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{dr(2^m-1)})+\mathrm{Tr}_1^2(x^{\frac{2^n-1}{3}})$$

If $f_{a_r,\beta}$ is hyper-bent then, $h_{a_r,1}$ is hyper-bent.

Proof. Set $h_0(x):=\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{dr(2^m-1)})$. One has (since $\gcd(d,2^m+1)=3$)

$$\sum_{v\in V}\chi(h_0(v))=\sum_{v\in V}\chi(f_0(v^d))=\sum_{v\in V}\chi(f_0(v^3))=\sum_{v\in V}\chi(f_0(v))$$

since the mapping $v\mapsto v^3$ is a permutation when $m\not\equiv 3 \pmod 6$. On the other hand, note that (since $\gcd(d,2^m+1)=3$)

$$\sum_{u\in U}\chi(h_0(u))=\sum_{u\in U}\chi(f_0(u^d))=\sum_{u\in U}\chi(f_0(u^3))=3\sum_{v\in V}\chi(f_0(v)).$$

Now, $\sum_{v\in V}\chi(f_0(v))=-1$ according to Lemma 6.2.4, since $f_{a_r,\beta}$ is hyper-bent. Hence, $2\sum_{v\in V}\chi(h_0(v))-\sum_{u\in U}\chi(h_0(u))=-2-(-3)=1$, proving that $h_{a_r,1}$ is hyper-bent (according to Lemma 6.2.4). □

The following theorem summarizes the study of the bentness of functions in $\mathfrak{H}_n$

Theorem 6.2.10. *([192]) Let $n=2m$ with m odd. Let $b\in\mathbb{F}_4^\star$ and β be a primitive element of $\mathbb{F}_4$. Let $f_{a_r,b}$ be a function of $\mathfrak{H}_n$ defined on $\mathbb{F}_{2^n}$ by (6.2). Let g_{a_r} be the related function defined on $\mathbb{F}_{2^m}$ by $g_{a_r}(x)=\sum_{r\in R}\mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r.*

1. *$f_{a_r,b}$ is hyper-bent if and only if $f_{a_r,b}$ is bent.*
2. *The bent functions $f_{a_r,b}$ are in the class $\mathcal{PS}^-$. Moreover, the bent functions $f_{a_r,b}$ are elements of the Partial Spread class $\mathcal{PS}_{ap}$ (resp. $\mathcal{PS}_{ap}^{\#}$) if $b=1$ (resp. if $b\neq 1$).*
3. *The three following assertions are equivalent:*
   (a) *$f_{a_r,\beta}$ is hyper-bent;*
   (b) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g_{a_r}(D_3(x))\Big)=-2;$
   (c) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+g_{a_r}(D_3(x))\Big)=2^m-2\,\mathrm{wt}(g_{a_r}\circ D_3)+4.$

4. $f_{a_r,1}$ is hyper-bent if and only if,
$2\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g_{a_r}(D_3(x))\Big)-3\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g_{a_r}(x)\Big)=2.$

Note that the previous theorem is valid when the coefficients a_r are elements of $\mathbb{F}_{2^m}$.

Problem 6.2.11. *Give an analogous characterization of functions of type (6.2) which are hyper-bent, in the case where some of the coefficients are in $\mathbb{F}_{2^n}$, but not in $\mathbb{F}_{2^m}$.*

Corollary 6.2.12 and Corollary 6.2.13 show that we can recover the results given in [195] and [196] using directly the characterizations given by Theorem 6.2.10.

Corollary 6.2.12. *([198]) Let $n=2m$ with m odd ($m>3$). Take in Theorem 6.2.10, $\#R=1$ and $r=1$. For simplicity, denote by a the coefficient a_1. Let f_{a,β^i} be the corresponding function (where β be a primitive element of $\mathbb{F}_4$, $i\in\{0,1,2\}$) defined on $\mathbb{F}_{2^n}$ by (6.2). Then, the function $f_{a,1}$ is not bent and, the function $f_{a,\beta}$ (resp. f_{a,β^2}) is hyper-bent whenever $K_m(a)=4$ while, when $K_m(a)\neq 4$, $f_{a,\beta}$ (resp. f_{a,β^2}) is not hyper-bent.*

Proof. According to Lemma 11 in [192], $f_{a,\beta}$ is hyper-bent if and only if f_{a,β^2} is hyper-bent. Moreover, according to Theorem 6.2.10, the function $f_{a,\beta}$ is hyper-bent if and only if

$$\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(1/x)=1}\chi(g_a(D_3(x)))=-2$$

where g_a is the the related function (defined in Theorem 6.2.10) which is equal to $\mathrm{Tr}_1^m(ax)$ (since the Dickson polynomial of degree 1 is equals X). The Dickson polynomial of degree 3 equals X^3+X thus,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(1/x)=1}\chi(g(D_3(x)))&=\sum_{x\in\mathbb{F}_{2^m}^\star}\chi(\mathrm{Tr}_1^m(a(x^3+x)))\\&-\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(1/x)=0}\chi(\mathrm{Tr}_1^m(a(x^3+x)))\\&=C_m(a,a)-1-\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(1/x)=0}\chi(\mathrm{Tr}_1^m(a(x^3+x)))\\&=C_m(a,a)-1-\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(1/x)=0}\chi(\mathrm{Tr}_1^m(ax)).\end{aligned}$$

In the last equality, we use the fact that the mapping $x\mapsto D_3(x):=x^3+x$ is a permutation on the set of $\mathbb{F}_{2^m}^\star$ such that $\mathrm{Tr}_1^m(1/x)=0$ (see *e.g.* [57, Lemma 7]).
Now, according to Charpin *et al.* [57],

$$\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(1/x)=0}\chi(\mathrm{Tr}_1^m(ax))=\frac{K_m(a)}{2}-1.$$

Hence, we get that

$$\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(1/x)=1}\chi(g(D_3(x)))=C_m(a,a)-\frac{K_m(a)}{2}.$$

Therefore, $f_{a,\beta}$ (resp. f_{a,β^2}) is hyper-bent if and only if $K_m(a)-2C_m(a,a)=4$. The mapping $x\mapsto x^3$ is a permutation on $\mathbb{F}_{2^m}$ for m odd, every element $a\in\mathbb{F}_{2^m}$ can be (uniquely) written as

$a = a'^3$ with $a' \in \mathbb{F}_{2^m}$. One has $C_m(a,a) = \sum_{x\in\mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^m((a'x)^3 + ax) = C_m(1, a^{2/3})$. Hence, according to Proposition 2.2.5 (note that $\mathrm{Tr}_1^m(a^{2/3}) = \mathrm{Tr}_1^m(a^{1/3})$), the function $f_{a,\beta}$ (resp. f_{a,β^2}) is hyper-bent if and only if,

$$K_m(a) = \begin{cases} 4 \text{ if } \mathrm{Tr}_1^m(a^{1/3}) = 0 \\ 4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2} \text{ if } \mathrm{Tr}_1^m(a^{1/3}) = 1 \end{cases}$$

However, using Proposition 2.2.2, the value $4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2}$ does not belong to $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$ for every $m > 3$. This proves that if $\mathrm{Tr}_1^m(a^{1/3}) = 0$, then the function $f_{a,\beta}$ (resp. f_{a,β^2}) is hyper-bent whenever $K_m(a) = 4$ while, when $K_m(a) \neq 4$, f_β (resp. f_{a,β^2}) is not hyper-bent. Otherwise, if $\mathrm{Tr}_1^m(a^{1/3}) = 1$ (which implies that $K_m(a) \neq 4$), then the function $f_{a,\beta}$ (resp. f_{a,β^2}) cannot be hyper-bent when $m > 3$. On the other hand, according to Theorem 6.2.10, $f_{a,1}$ is hyper-bent if and only if,

$$2 \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g_a(D_3(x))\Big) - 3 \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g_a(x)\Big) = 2.$$

We have seen that

$$\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(1/x)=1} \chi(g_a(D_3(x))) = C_m(a,a) - \frac{K_m(a)}{2}.$$

Furthermore, according to [57],

$$\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g_a(x)\Big) = \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(1/x)=1} \chi(\mathrm{Tr}_1^m(ax)) = -\frac{K_m(a)}{2}.$$

Therefore, $f_{a,1}$ is hyper-bent if and only if,

$$K_m(a) + 4C_m(a,a) = 4.$$

Recalling that $C_m(a,a) = C_m(1, a^{2/3})$ and Proposition 2.2.5, we get that $f_{a,1}$ is hyper-bent if and only if,

$$K_m(a) = \begin{cases} 4 \text{ if } \mathrm{Tr}_1^m(a^{1/3}) = 0 \\ 4 \pm \left(\frac{2}{m}\right) 2^{(m+5)/2} \text{ if } \mathrm{Tr}_1^m(a^{1/3}) = 1 \end{cases}$$

However, again by Proposition 2.2.2, the value $4 \pm \left(\frac{2}{m}\right) 2^{(m+5)/2}$ does not belong to $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$ for every $m > 3$. This proves that if $\mathrm{Tr}_1^m(a^{1/3}) = 0$, then the function $f_{a,1}$ is hyper-bent whenever $K_m(a) = 4$ while, when $K_m(a) \neq 4$, $f_{a,1}$ is not hyper-bent. Otherwise, if $\mathrm{Tr}_1^m(a^{1/3}) = 1$ (which implies that $K_m(a) \neq 4$), then the function $f_{a,1}$ cannot be hyper-bent when $m > 3$. □

Corollary 6.2.13. *([198]) Let $n = 2m$ with m odd such that $m \not\equiv 3 \pmod 6$. Take in Theorem 6.2.10, $\#R = 1$ and $r = 3$. For simplicity, denote by a the coefficient a_1. Let $f_{a,\beta}$ be the corresponding function (where β be a primitive element of $\mathbb{F}_4$) defined on $\mathbb{F}_{2^n}$ by (6.2). If $\mathrm{Tr}_1^m(a^{1/3}) = 0$ then, the function $f_{a,\beta}$ is hyper-bent whenever $K_m(a) = 4$ and if $\mathrm{Tr}_1^m(a^{1/3}) = 1$ then, the function $f_{a,\beta}$ is not hyper-bent.*

Proof. Since $m \not\equiv 3 \pmod 6$, the integers $\frac{2^m+1}{3}$ and 3 are co-prime. Applying Proposition 6.2.9 for $d = 3$ we obtain, $f_{a,\beta}$ is hyper-bent if and only if, the function $x \mapsto \mathrm{Tr}_1^n(ax^{(2^m-1)}) + \mathrm{Tr}_1^2(\beta x^{\frac{2^n-1}{3}})$ is hyper-bent. Now according to Corollary 6.2.12, we deduce that $f_{a,\beta}$ is hyper-bent whenever $K_m(a) = 4$ while, when $K_m(a) \neq 4$, f_β is not hyper-bent. Otherwise, if $\mathrm{Tr}_1^m(a^{1/3}) = 1$ (which implies that $K_m(a) \neq 4$) then, the function $f_{a,\beta}$ cannot be hyper-bent when $m > 3$. □

The extended Walsh-Hadamar transform of $f_{a,b}$[1] can be expressed as follows.

Proposition 6.2.14. *The notation is as in Theorem 6.2.10 except that we allow b to be equal to zero. In that specific case, we do not suppose m to be odd. Then*

$$\widehat{\chi_{f_{a,b}}}(0,k) = 1 + \Lambda(f_{a,b})\left(-1+2^m\right) \ ,$$

and, for $\omega \in \mathbb{F}_{2^n}^*$ non-zero,

$$\widehat{\chi_{f_{a,b}}}(\omega,k) = 1 - \Lambda(f_{a,b}) + 2^m(-1)^{f_{a,b}(\omega^{(2^m-1)/(2k)})} \ .$$

Proof. We denote by U the set of (2^m+1)-th roots of unity in $\mathbb{F}_{2^n}$. It is a well-known fact that every non-zero element $x \in \mathbb{F}_{2^n}^*$ has a unique polar decomposition as a product $x = yu$ where y lies in the subfield $\mathbb{F}_{2^m}$ and $u \in U$.

The extended Walsh–Hadamard transform of $f_{a,b}$ at (ω,k) can consequently be expressed as

$$\begin{aligned}
\widehat{\chi_{f_{a,b}}}(\omega,k) &= \sum_{x\in\mathbb{F}_{2^n}} \chi\left(f_{a,b}(x) + \mathrm{Tr}_1^n\left(\omega x^k\right)\right) \\
&= 1 + \sum_{x\in\mathbb{F}_{2^n}^*} \chi\left(f_{a,b}(x) + \mathrm{Tr}_1^n\left(\omega x^k\right)\right) \\
&= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(f_{a,b}(yu) + \mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \ .
\end{aligned}$$

But

$$\begin{aligned}
f_{a,b}(yu) &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r (yu)^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(b(yu)^{\frac{2^n-1}{3}}\right) \\
&= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r y^{r(2^m-1)} u^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(b y^{(2^m-1)\frac{2^m+1}{3}} u^{\frac{2^n-1}{3}}\right) \\
&= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r u^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(b u^{\frac{2^n-1}{3}}\right) \\
&= f_{a,b}(u) \ ,
\end{aligned}$$

so that

$$\begin{aligned}
\widehat{\chi_{f_{a,b}}}(\omega,k) &= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(f_{a,b}(u) + \mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \\
&= 1 + \sum_{u\in U}(-1)^{f_{a,b}(u)} \sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \\
&= 1 + \sum_{u\in U}(-1)^{f_{a,b}(u)} \left(-1 + \sum_{y\in\mathbb{F}_{2^m}} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right)\right) \ .
\end{aligned}$$

If $\omega = 0$, then $\widehat{\chi_f}(\omega,k) = 1 + \Lambda(f_{a,b})\left(-1+2^m\right)$ as desired. If $\omega \neq 0$, then one uses the

[1] For simplicity, we shall write from now $f_{a,b}$ instead of $f_{a_r,b}$

i=1	j= 0, 1, 2, 3, 5, 7, 8, 9, 11, 12, 13, 14, 17, 20, 22, 24, 26, 27, 29
i=2	j= 0, 2, 3, 4, 6, 9, 10, 13, 14, 16, 17, 18, 21, 22, 23, 24, 26, 27, 28
i=4	j= 0, 1, 3, 4, 5, 6, 8, 11, 12, 13, 15, 17, 18, 20, 21, 23, 25, 26, 28
i=7	j= 0, 3, 4, 5, 7, 8, 10, 11, 12, 14, 16, 18, 19, 23, 26, 27, 28, 29, 30
i=8	j= 0, 2, 3, 5, 6, 8, 9, 10, 11, 12, 15 16, 19, 21, 22, 24, 25, 26, 30,
i=14	j= 0, 1, 5, 6, 7, 8, 10, 14, 15, 16, 20, 21, 22, 23, 24, 25, 27, 28, 29
i=16	j= 0, 1, 4, 6, 7, 10, 11 12, 13, 16, 17, 18, 19, 20, 21, 22, 24, 29, 30
i=19	j= 0, 4, 5, 6, 7, 8, 9, 13, 14, 15, 17, 18, 19, 21, 25, 27, 29, 2, 30
i=25	j= 0, 1, 2, 3, 4, 7, 9, 15, 18, 19, 20, 22, 23, 24, 25, 26, 28, 29, 30
i=28	j= 0, 1, 2, 9, 10, 11, 12, 13, 14, 15 16, 17, 19, 20, 23, 25, 27, 28, 30

Table 6.1 – Exponents i and j such that (α^i, α^j) satisfy Conjecture 6.2.15 for $n = 10$

transitivity of the trace: $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(x)) = \mathrm{Tr}_1^m\left(x + x^{2^m}\right)$, which yields

$$\begin{aligned}\mathrm{Tr}_1^n\left(\omega y^k u^k\right) &= \mathrm{Tr}_1^m\left(\mathrm{Tr}_m^n\left(\omega y^k u^k\right)\right)\\ &= \mathrm{Tr}_1^m\left(\omega y^k u^k + \left(\omega y^k u^k\right)^{2^m}\right)\\ &= \mathrm{Tr}_1^m\left(\omega y^k u^k + \omega^{2^m} y^k u^{-k}\right)\\ &= \mathrm{Tr}_1^m\left(y^k\left(\omega u^k + \omega^{2^m} u^{-k}\right)\right) \quad .\end{aligned}$$

As k is co-prime with $2^m - 1$, the map $y \mapsto y^k$ is a permutation of $\mathbb{F}_{2^m}$ and the sum over $\mathbb{F}_{2^m}$ is non-zero if and only if $u^{2k} = \omega^{2^m-1}$. As k is co-prime with $2^m + 1$, this only occurs for a value of u and we get the final equality

$$\widehat{\chi_{f_{a,b}}}(\omega, k) = 1 - \Lambda(f_{a,b}) + 2^m(-1)^{f_{a,b}(\omega^{(2^m-1)/(2k)})} \quad . \qquad \square$$

6.2.1 Some conjectures: towards new hyper-bent functions

In the following, we make some conjectures that lead to construct new hyper-bent functions. To this end, we need to introduce some notation. Let $I := \{x \in \mathbb{F}_{2^m}^\star \mid x = c^3 + c, \mathrm{Tr}_1^m(c^{-1}) = 1\}$ and set, for a, $a' \in \mathbb{F}_{2^m}$,

$$\mathcal{S}(a, a') := \sum_{x \in I} (-1)^{\mathrm{Tr}_1^m(a(x+x^3)+a'x^5)}.$$

Conjecture 6.2.15. *For every $a \in \mathbb{F}_{2^m}^\star$, the set $\Gamma_a := \{a' \in \mathbb{F}_{2^m}^\star \mid \mathcal{S}(a, a') = -1\}$ is non empty.*

By a computer program, we have checked that Conjecture 6.2.15 holds for all $n = 2m$ up to $n = 26$ and for every $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$. Moreover, we have made an exhaustive search by a computer program for $n \in \{10, 14, 18, 22\}$ of all sets Γ_a for each value a such that $K_m(a) = 4$. Let ζ be a primitive element of $\mathbb{F}_{2^{10}}$ (whose minimal polynomial is $x^{10} + x^7 + 1$) and set $\alpha = \zeta^{33}$ (so that α is a primitive element of $\mathbb{F}_{2^5}$). We list in Table 6.1 all the pairs of indices (i, j) such that $K_5(\alpha^i) = 4$ and $\alpha^j \in \Gamma_{\alpha^i}$. We have also found all pairs (i, j) for $n \in \{14, 18, 22\}$. Due to their number, we do not list them like for $n = 10$ but we only give in Table III the numbers of pairs that we found (including the case where $K_m(a) = 4$ and $S(a, 0) = -1$).

Proposition 6.2.16. *([198]) Let $n = 2m$ with m odd. Suppose that Conjecture 6.2.15 holds. Let $a \in \mathbb{F}_{2^m}^\star$, $a' \in \Gamma_a$ ($\neq \emptyset$) and β is a primitive element of $\mathbb{F}_4$. Then, the function f the function defined on $\mathbb{F}_{2^n}$ by*

n	14	18	22
Number of pairs	882	3978	13948

Table 6.2 – Number of exponents such that (α^i, α^j) satisfy Conjecture 6.2.15 for $n \in \{14, 18, 22\}$

$$f(x) = \mathrm{Tr}_1^n((a+a')x^{3(2^m-1)}) + \mathrm{Tr}_1^n(a'x^{5(2^m-1)}) + \mathrm{Tr}_1^2(\beta x^{\frac{2^n-1}{3}})$$

is hyper-bent.

Proof. We denote by g be the function defined on $\mathbb{F}_{2^m}$ as

$$g(x) = \mathrm{Tr}_1^m((a+a')D_3(x)) + \mathrm{Tr}_1^m(a'D_5(x)).$$

Recall that $D_3(x) = x + x^3$ and, $D_5(x) = x + x^3 + x^5$. So $g(x) = \mathrm{Tr}_1^m\left(a(x+x^3) + a'x^5\right)$. Now, according to Theorem 6.2.10, f is hyper-bent if and only if, $\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g(D_3(x))) = -2$. Now, according to Charpin *et al.* [57] (Lemma 6), the mapping $x \mapsto D_3(x)$ is 3-to-1 from $\{x \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2 \mid \mathrm{Tr}_1^m(x^{-1}) = 1\}$ to $I := \{x \in \mathbb{F}_{2^m}^\star \mid x = c^3 + c, \mathrm{Tr}_1^m(c^{-1}) = 1\}$. Thus, the above condition of hyper-bentness can be reworded as

$$1 + 3\sum_{x\in I} \chi(g(x)) = -2 \text{ , that is, } \sum_{x\in I} \chi(g(x)) = -1.$$

The result follows.

□

More Generally, let set, for $(a, a') \in \mathbb{F}_{2^m}^\star$ and $a'' \in \mathbb{F}_{2^m}$,

$$\mathcal{S}'(a, a', a'') := \sum_{x\in I} (-1)^{\mathrm{Tr}_1^m(ax + a'x^3 + a''x^5)}$$

Conjecture 6.2.17. *The set* $\Gamma' := \{(a, a', a'') \in \mathbb{F}_{2^m}^\star \times \mathbb{F}_{2^m}^\star \times \mathbb{F}_{2^m} \mid \mathcal{S}'(a, a', a'') = -1\}$ *is not empty.*

By a computer search, we have found that for $n = 10$, there exist 1524 3-tuples $(a, a', a")$ such that $\mathcal{S}'(a, a', a'') = -1$, for $n = 14$, there exist 58790 such 3-tuples $(a, a', a")$ and, for $n = 18$, there exist 1904870 such 3-tuples $(a, a', a")$.

Proposition 6.2.18. *([198]) Let $n = 2m$ with m odd. Suppose that Conjecture 6.2.17 holds. Let $(a, a', a'') \in \Gamma'$ $(\neq \emptyset)$ and β is a primitive element of $\mathbb{F}_4$. Then, the function f defined on $\mathbb{F}_{2^n}$ by*

$$f(x) = \mathrm{Tr}_1^n((a+a')x^{2^m-1}) + \mathrm{Tr}_1^n((a'+a'')x^{3(2^m-1)}) + \mathrm{Tr}_1^n(a''x^{5(2^m-1)}) + \mathrm{Tr}_1^2(\beta x^{\frac{2^n-1}{3}})$$

is hyper-bent.

Proof. We denote g be function defined on $\mathbb{F}_{2^m}$ by

$$g(x) : = \mathrm{Tr}_1^m((a+a')D_1(x)) + \mathrm{Tr}_1^m((a'+a'')D_3(x)) + \mathrm{Tr}_1^m(a''D_5(x)).$$

According to the values of Dickson polynomial,

$$g(x) = \mathrm{Tr}_1^m\left((a+a')x\right) + \mathrm{Tr}_1^m\left((a'+a'')(x+x^3)\right) + \mathrm{Tr}_1^m\left(a''(x+x^3+x^5)\right)$$
$$= \mathrm{Tr}_1^m\left(ax + a'x^3 + a''x^5\right).$$

The mapping $x \mapsto D_3(x)$ is 3-to-1 from $\{x \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2 \mid \mathrm{Tr}_1^m(x^{-1}) = 1\}$ to $I := \{x \in \mathbb{F}_{2^m}^\star \mid x = c^3 + c, \mathrm{Tr}_1^m(c^{-1}) = 1\}$, therefore, the condition of hyper-bentness given by Theorem 6.2.10 can be reworded as

$$1 + 3\sum_{x\in I}\chi(g(x)) = -2, \text{ that is, } \sum_{x\in I}\chi(g(x)) = -1.$$

Equivalently,

$$\mathcal{S}'(a,a',a'') := \sum_{x\in I}(-1)^{\mathrm{Tr}_1^m(ax+a'x^3+a''x^5)} = -1.$$

The result follows. □

6.3 Hyper-bent functions with multiple trace terms via Dillon (like) expnents: the Wang et al. family

Adopting our approach presented in the previous section, Wang,Tang, Qi, Yang and Xu [258] have studied in late 2011 the following family with an additional trace term on $\mathbb{F}_{16}$:

$$f_{a,b}(x) = \sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right) \tag{6.6}$$

where the coefficients a_r lie in $\mathbb{F}_{2^m}$, the coefficient b is in $\mathbb{F}_{16}$ and m must verify $m \equiv 2 \pmod 4$ (the set R is defined as above ,that is, a subset of representatives of the cyclotomic cosets modulo 2^m+1 for which each coset has the maximal size n). We denote by $\mathfrak{W}_n$ the set of Boolean functions $f_{a,b}$ defined on $\mathbb{F}_{2^n}$ by (6.6).

We have provide a finer study of this family by giving results including useful expressions for their extended Walsh -Hadamard transform, their algebraic degrees and their duals.

The divisibility condition on m essentially entails that $2^m \equiv -1 \pmod 5$. A first consequence of this equality is that all functions in this family have the same algebraic degree, even the ones which are not hyper-bent.

Proposition 6.3.1. *([102]) Let $f_{a,b}$ be a function of $\mathfrak{W}_n$. The algebraic degree of the function $f_{a,b}$ is equal to m.*

Proof. The exponent 2^m-1 has 2-weight m since $2^m - 1 = 1 + 2 + 2^2 + \cdots + 2^{m-1}$. Moreover, $m \equiv 2 \pmod 4$ so that $n = 2m$ can be expressed as $n = 8l+4$. Then

$$\frac{2^n-1}{5} = \frac{16^{2l+1}-1}{5} = 3 \times \frac{16^{2l+1}-1}{15}$$
$$= 3 \times \sum_{i=0}^{2m} 16^i = \sum_{i=0}^{2l} 2^{4i} + \sum_{i=0}^{2l} 2^{4i+1} \ .$$

Therefore, the 2-weight of $\frac{2^n-1}{5}$ is $4l+2 = \frac{n}{2} = m$ as well.

Both Boolean functions $x \mapsto \sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)$ and $x \mapsto \mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$ are thus of algebraic degree m. Since they are separate parts in the trace representation of $f_{a,b}$, the algebraic degree of $f_{a,b}$ is equal to m as well. □

The divisibility condition on m also implies that $f_{a,b}(xy) = f_{a,b}(y)$ for any x in the subfield $\mathbb{F}_{2^m}$. The extended Walsh–Hadamard spectrum of $f_{a,b}$ can then be expressed with $\Lambda(f_{a,b})$ in a classical manner [170, Theorem 3], [101], thus extending the result of Wang et al. [258, Proposition 3.1] which gives a characterization of the hyper-bentness of $f_{a,b}$ using $\Lambda(f_{a,b})$ but does not provide an explicit expression for its extended Walsh–Hadamard spectrum.

Proposition 6.3.2. *([102]) Let $f_{a,b}$ be a function of $\mathfrak{W}_n$. Then*

$$\widehat{\chi_{f_{a,b}}}(0,k) = 1 + \Lambda(f_{a,b})\,(-1+2^m) \quad ,$$

and, for $\omega \in \mathbb{F}_{2^n}^*$ non-zero,

$$\widehat{\chi_{f_{a,b}}}(\omega,k) = 1 - \Lambda(f_{a,b}) + 2^m(-1)^{f_{a,b}(\omega^{(2^m-1)/(2k)})} \quad .$$

In particular, $f_{a,b}$ is hyper-bent if and only if $\Lambda(f_{a,b}) = 1$.

The dual of $f_{a,b}$ can then be explicitly computed when $f_{a,b}$ is hyper-bent.

Proposition 6.3.3. *([102]) If $f_{a,b}$ is hyper-bent, then its dual is f_{a,b^4}, i.e. we have*

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{f_{a,b}}}(\omega) = 2^m \chi_{f_{a,b^4}}(\omega).$$

Proof. Let $u \in U$ be the unique element such that $u^{1-2^m} = u^2 = \omega^{2^m-1}$, that is $u = \omega^{(2^m-1)/2}$. Then $f_{a,b}(u) = f_{a,b}(\omega^{-1})$.

Moreover, since $m \equiv 2 \pmod 4$, 15 divides $2^m - 4$. Hence, $b^{2^m} = b^4$ and it follows that $f_{a,b}(\omega^{-1}) = f_{a,b^4}(\omega)$. □

Extending our approach [197, 192], Wang et al. [258] derived the following characterization of the hyper-bentness property of such functions in two cases

- $b = 1$ and $b^4 + b + 1 = 0$
- $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$

They showed that hyper-bentness of these functions for the two cases are related to some character sums involving Dickson polynomials of degree r and 5. The following theorem summarizes their results.

Theorem 6.3.4. *([258]) Suppose $m := \frac{n}{2} \equiv 2 \pmod 4$. Let $R \subseteq E$ where E is a set of representatives of the cyclotomic classes modulo $2^n - 1$ for which each class has the full size n. For $b \in \mathbb{F}_{16}^\star$ and $a_r \in \mathbb{F}_{2^m}^\star$, we denote by $\tilde{g}_{a_r,b}$ the function defined on $\mathbb{F}_{2^n}$ by $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^4(b' x^{\frac{2^n-1}{5}})$, and by h_{a_r} the function defined on $\mathbb{F}_{2^m}$ by $\sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then,*

1. *If b a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$ then, $\sum_{u\in U} \chi\Big(\tilde{g}_{a_r,b}(u)\Big) = 1$ if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) = 2$$

2. *If $b = 1$ then, $\sum_{u\in U} \chi\Big(\tilde{g}_{a_r,1}(u)\Big) = 1$ if and only if*

$$2 \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) - 5 \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = 4.$$

3. *Assume* $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. *If* $b \in \{\beta, \beta^2, \beta^3, \beta^4\}$ *where* β *is a primitive 5-th root of unity in* $\mathbb{F}_{16}$ *then,* $\sum_{u\in U} \chi\Big(\tilde{g}_{a_r,b}(u)\Big) = 1$ *if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) + 5 \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = -8.$$

4. *Assume* $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. *If* b *is a primitive element of* $\mathbb{F}_{16}$ *such that* $\mathrm{Tr}_1^4(b) = 1$ *then,* $\sum_{u\in U} \chi\Big(\tilde{g}_{a_r,b}(u)\Big) = 1$ *if and only if,*

$$3 \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) - 5 \sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = -4.$$

5. *Assume* $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. *If* $b \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4, \beta+\beta^4, \beta^2+\beta^3\}$ *where* β *is a primitive 5-th root of unity in* $\mathbb{F}_{16}$ *then,* $\sum_{u\in U} \chi\Big(\tilde{g}_{a_r,b}(u)\Big) = 1$ *if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) = 2.$$

We deduced the following expressions for $\Lambda(f_{a,b})$.

Theorem 6.3.5. *Suppose* $m := \frac{n}{2} \equiv 2 \pmod 4$. *Let* $R \subseteq E$ *where* E *is a set of representatives of the cyclotomic classes modulo* $2^n - 1$ *for which each class has the full size* n. *For* $b \in \mathbb{F}_{16}^\star$ *and* $a_r \in \mathbb{F}_{2^m}^\star$, *we denote by* $\tilde{g}_{a_r,b}$ *the function defined on* $\mathbb{F}_{2^n}$ *by* $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^4(b' x^{\frac{2^n-1}{5}})$, *and by* g_a *the function defined on* $\mathbb{F}_{2^m}$ *by* $\sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, *where* $D_r(x)$ *is the Dickson polynomial of degree* r. *Then,*

1. *If* $b = 1$, *then* $5\Lambda(f_{a,1}) = 4T_1^5(g_a) - 10T_1(g_a) - 3$.
2. *If* b *is a primitive element of* $\mathbb{F}_{16}$ *such that* $\mathrm{Tr}_1^4(b) = 0$, *then* $5\Lambda(f_{a,b}) = 2T_1^5(g_a) + 1$.
3. *If moreover* $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$, *then*
   (a) *if* b *is a primitive element of* $\mathbb{F}_{16}$ *such that* $\mathrm{Tr}_1^4(b) = 1$, *then* $5\Lambda(f_{a,b}) = -3T_1^5(g_a) + 5T_1(g_a) + 1$;
   (b) *if* b *is a primitive* 5*-th root of unity, then* $5\Lambda(f_{a,b}) = -T_1^5(g_a) - 5T_1(g_a) - 3$;
   (c) *if* b *is a primitive* 3*-rd root of unity, then* $5\Lambda(f_{a,b}) = 2T_1(g_a) + 1$.

Recall that $f_{a,b}$ is hyper-bent if and only if $\Lambda(f_{a,b}) = 1$. Therefore, the above theorem gives a characterization of the hyper-bentness of $f_{a,b}$ using $T_1^5(g_a)$ and $T_1(g_a)$. These exponential sums can then be reformulated in terms of the Hamming weight of g_a and related functions using Lemma 2.4.8.

6.4 Hyper-bent functions via Dillon-like exponents: the general study

In this section, we shall use the notation Subsection 2.2.3 dealing with partial exponential sums.

6.4.1 Extending the Charpin–Gong criterion

The family of Boolean functions $\mathcal{F}_n$ consists of the functions f_a given in trace representation by Dillon-like only exponents, that is

$$f_a(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) \tag{6.7}$$

where R is a set of representatives of the cyclotomic classes modulo $2^m + 1$ (hence the elements $r(2^m - 1)$ yield a set of representatives of the cyclotomic classes modulo $2^n - 1$ of the form $[i(2^m - 1)]$) and the coefficients a_r live in the field $\mathbb{F}_{2^n}$. Departing from the approach of Charpin and Gong, we do not require that the cyclotomic cosets are of maximal size $n = 2m$.

Lemma 6.4.1. *Let f_a be a Boolean function in $\mathcal{F}_n$. Then $f_a(\alpha^{2^m+1}x) = f_a(x)$.*

Proof. We indeed have

$$\begin{aligned} f_a(\alpha^{2^m+1}x) &= \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r (\alpha^{2^m+1}x)^{r(2^m-1)} \right) \\ &= \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r \alpha^{r(2^n-1)} x^{r(2^m-1)} \right) \\ &= f_a(x) \ . \end{aligned}$$

□

Proposition 5.4.2 can therefore be directly applied to characterize the hyper-bentness of f_a with the partial exponential sum $\Lambda(a) = \Lambda(f_a)$.

Proposition 6.4.2. *Let f_a be a Boolean function in $\mathcal{F}_n$. The function f_a is hyper-bent if and only if $\Lambda(a) = 1$.*

Proof. According to Proposition 5.4.2, f_a is hyper-bent if and only if its restriction to U has Hamming weight 2^{m-1}. Moreover, we have $\Lambda(a) = \#U - 2\,\mathrm{wt}(f_a|_U) = 2^m + 1 - 2\,\mathrm{wt}(f_a|_U)$. Thus, f_a is hyper-bent if and only if $\Lambda(a) = 1$. □

Remark 6.4.3. *A hyper-bent function $f_a \in \mathcal{F}_n$ is in $\mathcal{PS}_{ap}$ if and only if $\sum_{r \in R} \mathrm{Tr}_1^n(a_r) = 1$.*

In fact, the complete extended Walsh–Hadamard spectrum of f_a can be expressed with $\Lambda(a)$.

Proposition 6.4.4. *Let f_a be a Boolean function in $\mathcal{F}_n$ and k an integer co-prime with $2^n - 1$. For $\omega = 0$,*

$$\widehat{\chi_{f_a}}(0, k) = 1 + \Lambda(a)\,(-1 + 2^m) \ ,$$

and, for $\omega \in \mathbb{F}_{2^n}^*$ non-zero,

$$\widehat{\chi_{f_a}}(\omega, k) = 1 - \Lambda(a) + 2^m \chi_{f_a}\left(\omega^{(2^m-1)/(2k)} \right) \ .$$

Proof. It is a well-known fact that every non-zero element $x \in \mathbb{F}_{2^n}^*$ has a unique polar decomposition as a product $x = yu$ where y lies in the subfield $\mathbb{F}_{2^m}$ and $u \in U$.

The extended Walsh–Hadamard transform of f_a at (ω, k) can consequently be expressed as

$$\begin{aligned} \widehat{\chi_{f_a}}(\omega, k) &= \sum_{x \in \mathbb{F}_{2^n}} \chi\left(f_a(x) + \mathrm{Tr}_1^n\left(\omega x^k\right)\right) \\ &= 1 + \sum_{x \in \mathbb{F}_{2^n}^*} \chi\left(f_a(x) + \mathrm{Tr}_1^n\left(\omega x^k\right)\right) \\ &= 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^*} \chi\left(f_a(yu) + \mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \ . \end{aligned}$$

But

$$\begin{aligned} f_a(yu) &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r(yu)^{r(2^m-1)}\right) \\ &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r y^{r(2^m-1)}u^{r(2^m-1)}\right) \\ &= \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r u^{r(2^m-1)}\right) \\ &= f_a(u) \ , \end{aligned}$$

so that

$$\begin{aligned} \widehat{\chi_{f_a}}(\omega,k) &= 1+\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(f_a(u)+\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \\ &= 1+\sum_{u\in U}\chi_{f_a}(u)\sum_{y\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \\ &= 1+\sum_{u\in U}\chi_{f_a}(u)\left(-1+\sum_{y\in\mathbb{F}_{2^m}} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right)\right) \\ &= 1-\Lambda(a)+\sum_{u\in U}\chi_{f_a}(u)\sum_{y\in\mathbb{F}_{2^m}} \chi\left(\mathrm{Tr}_1^n\left(\omega y^k u^k\right)\right) \ . \end{aligned}$$

If $\omega = 0$, then $\widehat{\chi_f}(\omega,k) = 1+\Lambda(a)\left(-1+2^m\right)$ as desired.
If $\omega \neq 0$, then the transitivity of the trace yields

$$\begin{aligned} \mathrm{Tr}_1^n\left(\omega y^k u^k\right) &= \mathrm{Tr}_1^m\left(\mathrm{Tr}_m^n\left(\omega y^k u^k\right)\right) \\ &= \mathrm{Tr}_1^m\left(\omega y^k u^k+\left(\omega y^k u^k\right)^{2^m}\right) \\ &= \mathrm{Tr}_1^m\left(\omega y^k u^k+\omega^{2^m} y^k u^{-k}\right) \\ &= \mathrm{Tr}_1^m\left(y^k\left(\omega u^k+\omega^{2^m}u^{-k}\right)\right) \ . \end{aligned}$$

As a consequence of this equality and of the fact that k is co-prime with 2^m-1, the sum over $\mathbb{F}_{2^m}$ is non-zero if and only if $u^{2k}=\omega^{2^m-1}$. As k is co-prime with 2^m+1, this only occurs for a value of u. Therefore

$$\widehat{\chi_{f_a}}(\omega,k) = 1-\Lambda(a)+2^m\chi_{f_a}\left(\omega^{(2^m-1)/(2k)}\right) \ . \qquad \square$$

In particular, Proposition 6.4.2 is a direct corollary to the above proposition.

Remark 6.4.5. *Set*

$$\overline{f}_a(x) = \sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^r\right) \ ,$$

and let $\overline{\Lambda}(a)=\Lambda(\overline{f}_a)$. *The integers* 2^m-1 *and* 2^m+1 *are co-prime and so the* (2^m-1)*-power map induces a permutation of* U. *In particular, one has* $\Lambda(a)=\overline{\Lambda}(a)$.

We now restrict to the family $\mathcal{G}_n$ of Boolean functions defined as above, but where the coefficients a_r are restricted to the subfield $\mathbb{F}_{2^m}$. The following remark shows that it is enough to restrict to Dillon-like exponents whose cyclotomic coset sizes do not divide m.

Remark 6.4.6. *If $t = o(r(2^m-1))$, then*

$$\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) = \mathrm{Tr}_1^t\left(\mathrm{Tr}_t^n\left(a_r\right) x^{r(2^m-1)}\right) \ .$$

Suppose now that $a_r \in \mathbb{F}_{2^m}$, e.g. *$f_a \in \mathcal{G}_n$. If t divides m, then $\mathrm{Tr}_t^n\left(a_r\right) = \mathrm{Tr}_t^m\left(a_r + a_r^{2^m}\right) = 0$ and*

$$\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) = 0 \ .$$

Otherwise, if $k = \gcd(t,m)$, then $\mathrm{Tr}_t^n\left(a_r\right) \in \mathbb{F}_{2^k}$.

Furthermore, Proposition 6.4.4 can be used to compute the dual of f_a in the case where f_a is hyper-bent.

Proposition 6.4.7. *Suppose that $f_a \in \mathcal{G}_n$ is hyper-bent. Then it is its own dual, i.e. we have*

$$\widehat{\chi_{f_a}}(\omega) = 2^m \chi_{f_a}(\omega) \ .$$

Proof. If f_a is hyper-bent, then $\Lambda(a) = 1$ and one has

$$\widehat{\chi_{f_a}}(\omega) = 2^m \chi_{f_a}(u) \ ,$$

where $u^{1-2^m} = \omega^{2^m-1}$. In particular, one has $f_a(u) = f_a(\omega^{-1})$. One then concludes that $f_a(\omega^{-1}) = f_a(\omega)$ using the facts that $a_r^{2^m} = a_r$ and that $2^m(1-2^m) \equiv 2^m - 1 \pmod{2^n-1}$. □

For functions f_a in $\mathcal{G}_n$, Remark 6.4.5 combined with the transitivity of the trace yields a useful expression of $\Lambda(a)$ using the partial exponential sum T_1 whose proof we recall here.

Lemma 6.4.8 ([192, Lemma 12])**.** *Let f_a be a Boolean function in $\mathcal{G}_n$ and l be any positive integer. Let g_a be the Boolean function defined on $\mathbb{F}_{2^m}$ as $g_a(x) = \sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_r(x)\right)$. Then $\Lambda(f_a(x^l)) = 1 + 2T_1(g_a \circ D_l)$.*

Proof. Using the facts that the (2^m-1)-power map induces a permutation of U, that $a_r^{2^m} = a_r$ and that $D_r(x + x^{-1}) = x^r + x^{-r}$ for any $x \in \mathbb{F}_{2^n}$, one gets

$$\begin{aligned}
\Lambda(f_a(x^l)) &= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r\left(u^{2^m-1}\right)^{lr}\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r u^{lr}\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(\left(a_r u^{lr}\right) + \left(a_r u^{lr}\right)^{2^m}\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r\left(u^{lr} + u^{-lr}\right)\right)\right) \\
&= \sum_{u\in U} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_r(D_l(u + u^{-1}))\right)\right) \ .
\end{aligned}$$

To conclude, recall that the map $x \mapsto x + x^{-1}$ is 2-to-1 from $U \setminus \{1\}$ to $\mathcal{T}_1$ to obtain

$$\begin{aligned}
\Lambda(f_a(x^l)) &= 1 + 2\sum_{t\in\mathcal{T}_1} g_a(D_l(t)) \\
&= 1 + 2T_1(g_a \circ D_l) \ .
\end{aligned}$$

□

The following extension of the Charpin–Gong criterion ([54], Theorem 7) is then straightforward.

Theorem 6.4.9. *Let f_a be a Boolean function in $\mathcal{G}_n$. Let g_a be the Boolean function defined on $\mathbb{F}_{2^m}$ as $g_a(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$. Then f_a is hyper-bent if and only if $T_1(g_a) = 0$. Moreover, if f_a is hyper-bent, then it is in the $\mathcal{PS}_{ap}$ class.*

Proof. This is a direct consequence of Proposition 6.4.2 and Lemma 6.4.8. □

6.4.2 Hyper-bentness criterion for functions in $\mathcal{H}_n$

The above approach yields criteria for hyper-bentness of Boolean functions f_a in the families $\mathcal{F}_n$, respectively $\mathcal{G}_n$, involving only one exponential sum over $U \subset \mathbb{F}_{2^n}$, respectively $\mathcal{T}_1 \subset \mathbb{F}_{2^m}$.

In particular, applying Lemma 2.4.8 to Theorem 6.4.9, one gets a characterization for the hyper-bentness of $f_a \in \mathcal{G}_n$ involving only complete exponential sums over $\mathbb{F}_{2^m}$, or equivalently the Hamming weights of g_a and the related function $x \mapsto \mathrm{Tr}_1^m(1/x) + g_a(x)$ defined over $\mathbb{F}_{2^m}$.

Nonetheless, the restriction that lies on the coefficients a_r in the latter case is not satisfying, namely they should live in the field $\mathbb{F}_{2^n}$ rather than in $\mathbb{F}_{2^m}$. In this subsection, we extend our approach to partially address this issue, that is allow an additional trace term without any restriction on its coefficient.

We therefore consider a different family of Boolean functions defined as follows. The family of Boolean functions $\mathcal{H}_n$ consists of the functions $f_{a,b}$ defined as

$$f_{a,b}(x) = \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^t\left(b x^{s(2^m-1)}\right) \tag{6.8}$$

where R is a set of representatives of the cyclotomic classes modulo 2^m+1, the coefficients a_r are in $\mathbb{F}_{2^m}$, s divides 2^m+1, i.e. $s(2^m-1)$ is a Dillon-like exponent, $t = o(s(2^m-1))$, i.e. t is the size of the cyclotomic coset of s modulo 2^m+1, and the coefficient b is in $\mathbb{F}_{2^t}$. Moreover, let $\tau = \frac{2^m+1}{s}$. Remark that $f_{a,0} = f_a$ where $f_a \in \mathcal{G}_n$ is the function defined in the previous subsection. Set

$$\overline{f}_{a,b}(x) = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^r) + \mathrm{Tr}_1^t(b x^s) \quad .$$

Remark 6.4.10. *According to Remark 6.4.6, the family $\mathcal{H}_n$ is always strictly larger than the family $\mathcal{G}_n$.*

Let $U = \left\{u \in \mathbb{F}_{2^n}^* \mid u^{2^m+1} = 1\right\}$ be the subgroup of $\mathbb{F}_{2^n}^*$ of order 2^m+1, $V = \{v \in \mathbb{F}_{2^n}^* \mid v^s = 1\}$ its subgroup of order s and $W = \{w \in \mathbb{F}_{2^n}^* \mid w^\tau = 1\}$ its subgroup of order τ. Denote by α a primitive element of $\mathbb{F}_{2^n}$. Then $\zeta = \alpha^{2^m-1}$ is a generator of U, $\rho = \zeta^\tau$ is a generator of V and $\xi = \zeta^s$ is a generator of W.

Remark 6.4.11. *Note that $\mathbb{F}_{2^t}^* \supset W$. Indeed, by definition $s(2^m-1) \equiv 2^t s(2^m-1) \pmod{2^n-1}$. Thus, $(2^t-1)s \equiv 0 \pmod{2^m+1}$, which implies that $2^t-1 \equiv 0 \pmod{\tau}$, that is τ divides 2^t-1.*

Remark 6.4.12. *Let us consider the τ-power homomorphism $\phi : x \in \mathbb{F}_{2^n}^* \mapsto x^\tau \in \mathbb{F}_{2^n}^*$. Its kernel is W and so it is τ-to-1.*

Furthermore, V and W are subsets of U, so that the restriction of ϕ to U maps U onto V and is again τ-to-1.

A similar statement is clearly true for s, exchanging the sets V and W.

Remark 6.4.13. *The set U can be decomposed as*

$$U = \bigcup_{i=0}^{\tau-1} \zeta^i V = \bigcup_{i=0}^{s-1} \zeta^i W \ .$$

Definition 6.4.14. *For $i \in \mathbb{Z}$, define $S_i(a)$ and $\overline{S}_i(a)$ to be the partial exponential sums*

$$S_i(a) = \sum_{v \in V} \chi\left(f_a(\zeta^i v)\right) \ ,$$
$$\overline{S}_i(a) = \sum_{v \in V} \chi\left(\overline{f}_a(\zeta^i v)\right) \ .$$

Moreover, define $\Lambda(a,b) = \Lambda(f_{a,b})$ and $\overline{\Lambda}(a,b) = \Lambda(\overline{f}_{a,b})$.

Remark 6.4.15. *The Boolean function $f_{a,b}$ is hyper-bent if and only if $\Lambda(a,b) = 1$. Moreover, Remark 6.4.5 can be extended to $f_{a,b}$ and $\overline{f}_{a,b}$ and yields $\Lambda(a,b) = \overline{\Lambda}(a,b)$. Finally, Proposition 6.4.7 can be extended to show that, if $f_{a,b}$ is hyper-bent, then its dual is $f_{a,b^{2^m}}$.*

Remark 6.4.16. *Remark that ζ is of order τ so that $S_i(a)$ and $\overline{S}_i(a)$ only depend on the value of i modulo τ.*

Remark 6.4.17. *One obviously has*

$$\sum_{i=0}^{\tau-1} S_i(a) = \Lambda(a,0) = \Lambda(a) \ .$$

In particular, Lemma 6.4.8 yields

$$\sum_{i=0}^{\tau-1} S_i(a) = 1 + 2T_1(g_a) \ .$$

In the particular case where f_a is a monomial function with a Dillon exponent, i.e. $f_a(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$ where r is co-prime with 2^m+1, Remark 6.4.17 can be further refined.

Lemma 6.4.18. *Suppose that r is co-prime with 2^m+1. One has*

$$\sum_{i=0}^{\tau-1} S_i(a) = 1 - K_m(a) \ .$$

Proof. The function $u \mapsto u + u^{-1}$ being onto and 2-to-1 from $U \setminus \{1\}$ to $\mathcal{T}_1$, one gets

$$\begin{aligned} K_m(a) &= -2T_1(\mathrm{Tr}_1^m(ax)) \\ &= -\sum_{u \in U,\ u \neq 1} \chi\left(\mathrm{Tr}_1^m\left(a\left(u + u^{-1}\right)\right)\right) \\ &= -\sum_{u \in U,\ u \neq 1} \chi\left(\mathrm{Tr}_1^n(au)\right) \\ &= 1 - \sum_{u \in U} \chi\left(\mathrm{Tr}_1^n(au)\right) \ . \end{aligned}$$

Furthermore, the r-power map induces a permutation of U and thus

$$\begin{aligned}\sum_{u\in U}\chi\left(\mathrm{Tr}_1^n\left(au\right)\right) &= \sum_{u\in U}\chi\left(\mathrm{Tr}_1^n\left(au^r\right)\right)\\ &= \overline{\Lambda}(a)\\ &= \Lambda(a)\ .\end{aligned}$$

□

The two partial exponential sums S_i and $\overline{S}_i$ defined above are closely related.

Lemma 6.4.19. *For $0 \leq i \leq \tau - 1$, one has*

$$S_i(a) = \overline{S}_{-2i}(a)\ .$$

Proof. First, one has

$$\begin{aligned}S_i(a) &= \sum_{v\in V}\chi\left(f_a(\zeta^i v)\right)\\ &= \sum_{v\in V}\chi\left(\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r\left(\zeta^i v\right)^{r(2^m-1)}\right)\right)\\ &= \sum_{v\in V}\chi\left(\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r\left(\zeta^{i(2^m-1)}v^{2^m-1}\right)^r\right)\right)\ .\end{aligned}$$

But $2^m - 1$ is co-prime with s, so that the (2^m-1)-power map induces a permutation of V, as does multiplication by ζ^τ. Moreover, $2^m + 1 \equiv 0 \pmod{\tau}$ implies that $2^m - 1 \equiv -2 \pmod{\tau}$. Hence,

$$S_i(a) = \sum_{v\in V}\chi\left(\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r\left(\zeta^{-2i}v\right)^r\right)\right)\ .$$

□

Remark 6.4.17 can then be extended to express $\Lambda(a,b)$ as a linear combination of the sums S_i.

Proposition 6.4.20. *One has*

$$\Lambda(a,b) = \sum_{i=0}^{\tau-1}\chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right)\overline{S}_i(a)\ .$$

Proof. Indeed,

$$\begin{aligned}\Lambda(a,b) &= \overline{\Lambda}(a,b)\\ &= \sum_{u\in U}\chi\left(\overline{f}_a(u) + \mathrm{Tr}_1^t\left(bu^s\right)\right)\\ &= \sum_{u\in U}\chi\left(\overline{f}_a(u)\right)\chi\left(\mathrm{Tr}_1^t\left(bu^s\right)\right)\\ &= \sum_{i=0}^{\tau-1}\sum_{v\in V}\chi\left(\overline{f}_a(\zeta^i v)\right)\chi\left(\mathrm{Tr}_1^t\left(b\left(\zeta^i v\right)^s\right)\right)\\ &= \sum_{i=0}^{\tau-1}\chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right)\sum_{v\in V}\chi\left(\overline{f}_a(\zeta^i v)\right)\\ &= \sum_{i=0}^{\tau-1}\chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right)\overline{S}_i(a)\ .\end{aligned}$$

□

We now devise an additional relation between the partial exponential sums S_i and the partial exponential sum T_1. In particular, we express the partial exponential sum S_0 using T_1.

Lemma 6.4.21. *Let l be a divisor of τ and let k be the integer $k = \tau/l$. Then*

$$\sum_{i=0}^{k-1} S_{il}(a) = \sum_{i=0}^{k-1} \overline{S}_{il}(a) = \frac{1}{l}\left(1 + 2T_1(g_a \circ D_l)\right) \ .$$

For $l = 1$, it reads

$$\sum_{i=0}^{\tau-1} S_i(a) = \sum_{i=0}^{\tau-1} \overline{S}_i(a) = \left(1 + 2T_1(g_a)\right) \ ,$$

which is nothing but Remark 6.4.17. For $l = \tau$, it reads

$$S_0(a) = \overline{S}_0(a) = \frac{1}{\tau}\left(1 + 2T_1(g_a \circ D_\tau)\right) \ .$$

Proof. According to a straightforward extension of Remark 6.4.11, the l-power map is l-to-1 from U onto $\bigcup_{i=0}^{k-1} \zeta^{il} V$. Therefore,

$$\begin{aligned}\sum_{i=0}^{k-1} S_{il}(a) &= \sum_{i=0}^{k-1} \sum_{v \in V} \chi\left(f_a(\zeta^{il} v)\right) \\ &= \frac{1}{l} \sum_{u \in U} \chi\left(f_a(u^l)\right) \ .\end{aligned}$$

One then concludes with Lemma 6.4.8.

The results for $\overline{S}_i$ readily follows from the fact multiplication by -2 induces a permutation of $\{il\}_{i=0}^{k-1}$ and Lemma 6.4.19. □

Remark 6.4.22. *Recall that τ divides $2^m + 1$, and so does l. Therefore, τ and l are co-prime with $2^m - 1$. According to Corollary 2.4.6, D_l induces a permutation of $\mathcal{T}_0$, whence the validity of the equality*

$$\sum_{i=0}^{k-1} S_{il}(a) = \sum_{i=0}^{k-1} \overline{S}_{il}(a) = \frac{1}{l}\left(1 + 2\Xi\left(g_a \circ D_l\right) - 2T_0(g_a)\right) \ .$$

In the case where $l = \tau$, it reads

$$S_0(a) = \overline{S}_0(a) = \frac{1}{\tau}\left(1 + 2\Xi\left(g_a \circ D_\tau\right) - 2T_0(g_a)\right) \ .$$

To conclude this section, we show how further identities involving the partial exponential sums S_i can be obtained by restricting the field of definition of the coefficients a_r to a strict subfield of $\mathbb{F}_{2^m}$.

Lemma 6.4.23. *Let l be a divisor of m and $k = m/l$. Suppose that the coefficients a_r lie in $\mathbb{F}_{2^l}$ and that $2^l \equiv j \pmod{\tau}$, where j is a k-th root of -1 modulo τ. Then*

$$\overline{S}_i(a) = \overline{S}_{ij}(a) \ .$$

Proof. Recall that $2^m \equiv -1 \pmod{\tau}$. Hence, if $2^l \equiv j \pmod{\tau}$, then j is a k-th root of -1 modulo τ.

Since $a_r \in \mathbb{F}_{2^l}$, one has $a_r^{2^l} = a_r$. Recall that $\mathrm{Tr}_1^n\left(x^2\right) = \mathrm{Tr}_1^n(x)$, so that

$$\begin{aligned}\overline{S}_i(a) &= \sum_{v\in V} \chi\left(\overline{f}_a(\zeta^i v)\right)\\ &= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r(\zeta^i v)^r\right)\right)\\ &= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r^{2^l}(\zeta^{2^l i} v^{2^l})^r\right)\right)\\ &= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r(\zeta^{ij}\zeta^{i(2^l-j)} v^{2^l})^r\right)\right) \ .\end{aligned}$$

But the (2^l)-power map and multiplication by $\zeta^{i(2^l-j)}$ induce permutations of V and therefore

$$\begin{aligned}\overline{S}_i(a) &= \sum_{v\in V} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^n\left(a_r(\zeta^{ij} v)^r\right)\right)\\ &= \overline{S}_{ij}(a) \ .\end{aligned}$$

□

Remark 6.4.24. *In the particular case where $l = m$, note that $2^m \equiv -1 \pmod{\tau}$. Therefore, one has*

$$\overline{S}_i(a) = \overline{S}_{-i}(a) \ .$$

One then deduces from Proposition 6.4.20 that

$$\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^t(b)\right)\overline{S}_0(a) + \sum_{i=1}^{\frac{\tau-1}{2}} \left(\chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right) + \chi\left(\mathrm{Tr}_1^t\left(b\xi^{-i}\right)\right)\right)\overline{S}_i(a) \ .$$

Remark 6.4.25. *It is a difficult problem to deduce a completely general characterization of hyper-bentness in terms of complete exponential sums from the results of the current section, that is a characterization valid for any m, s and b. Nevertheless, several powerful applications of these results, valid for infinite families of Boolean functions, will be described in Section 6.6.*

6.4.3 An alternate proof

To provide an alternate proof of Proposition 6.4.20, we introduce different exponential sums.

Proposition 6.4.26. *For $c \in \mathbb{F}_{2^t}$, let $\widetilde{\Lambda}(a,c)$ be the exponential sum*

$$\widetilde{\Lambda}(a,c) = \sum_{b\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right)\Lambda(a,b) \ .$$

1. *For all $c \in \mathbb{F}_{2^t}$, one has*
$$\widetilde{\Lambda}(a,c) = 2^t \sum_{u\in U,\ u^s=c} \chi\left(\overline{f}_a(u)\right) \ .$$

2. *If $c \in \mathbb{F}_{2^t} \setminus W$, then $\widetilde{\Lambda}(a,c) = 0$. If $c \in W$, that is if $c = \xi^i$ for some i, then*
$$\widetilde{\Lambda}(a,\xi^i) = 2^t\overline{S}_i(a) \ .$$

Proof. 1. Exchanging the summation orders on U and $\mathbb{F}_{2^t}$ yields

$$\begin{aligned}\widetilde{\Lambda}(a,c) &= \sum_{b\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \sum_{u\in U} \chi\left(f_{a,b}(u)\right) \\ &= \sum_{b\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \sum_{u\in U} \chi\left(f_a(u)\right) \chi\left(\mathrm{Tr}_1^t\left(bu^{s(2^m-1)}\right)\right) \\ &= \sum_{u\in U} \chi\left(f_a(u)\right) \sum_{b\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t\left(b\left(c+u^{s(2^m-1)}\right)\right)\right) \ .\end{aligned}$$

The sum over $\mathbb{F}_{2^t}$ is non-zero if and only if $c = u^{s(2^m-1)}$ so that

$$\begin{aligned}\widetilde{\Lambda}(a,c) &= 2^t \sum_{u\in U,\ u^{s(2^m-1)}=c} \chi\left(f_a(u)\right) \\ &= 2^t \sum_{u\in U,\ u^s=c} \chi\left(\overline{f}_a(u)\right) \ .\end{aligned}$$

2. According to Remark 6.4.11, if $c \in \mathbb{F}_{2^t} \setminus W$, then the equation $u^s = c$ has no solutions in U. Therefore, we have $\widetilde{\Lambda}(a,c) = 0$.

   Suppose now that $c \in W$ and that $c = \xi^i = \zeta^{is}$ for some i. The kernel of the s-power map is V so that $u^s = \zeta^{is}$ if and only if $u \in \zeta^i V$. Thus, we have

$$\widetilde{\Lambda}(a,c) = 2^t \sum_{v\in V} \chi\left(\overline{f}_a(\zeta^i v)\right) \ . \qquad \square$$

The partial exponential sum $\Lambda(a,b)$ can now be expressed with $\widetilde{\Lambda}(a,c)$.

Lemma 6.4.27. *One has*

$$\Lambda(a,b) = \frac{1}{2^t} \sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) \ .$$

Proof. Going back to the definition of $\widetilde{\Lambda}(a,c)$, one has

$$\begin{aligned}\sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) &= \sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \sum_{d\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(dc)\right) \Lambda(a,d) \\ &= \sum_{d\in\mathbb{F}_{2^t}} \Lambda(a,d) \sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \chi\left(\mathrm{Tr}_1^t(dc)\right) \\ &= \sum_{d\in\mathbb{F}_{2^t}} \Lambda(a,d) \sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t((b+d)c)\right) \ .\end{aligned}$$

But $\sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t((b+d)c)\right) = 0$ if $b \neq d$ and 2^t otherwise. Therefore

$$\sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right) \widetilde{\Lambda}(a,c) = 2^t \Lambda(a,b) \ . \qquad \square$$

Remark 6.4.28. *Proposition 6.4.26 and Lemma 6.4.27 provide an alternate proof of Proposition 6.4.20:*

$$\begin{aligned}
\Lambda(a,b) &= \frac{1}{2^t}\sum_{c\in\mathbb{F}_{2^t}} \chi\left(\mathrm{Tr}_1^t(bc)\right)\widetilde{\Lambda}(a,c)\\
&= \frac{1}{2^t}\left(\sum_{c\in\mathbb{F}_{2^t}\setminus W} \chi\left(\mathrm{Tr}_1^t(bc)\right)\widetilde{\Lambda}(a,c) + \sum_{c\in W} \chi\left(\mathrm{Tr}_1^t(bc)\right)\widetilde{\Lambda}(a,c)\right)\\
&= \frac{1}{2^t}\sum_{c\in W} \chi\left(\mathrm{Tr}_1^t(bc)\right)\widetilde{\Lambda}(a,c)\\
&= \frac{1}{2^t}\sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right)\widetilde{\Lambda}(a,\xi^i)\\
&= \frac{1}{2^t}\sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right)2^t\overline{S}_i(a)\\
&= \sum_{i=0}^{\tau-1} \chi\left(\mathrm{Tr}_1^t\left(b\xi^i\right)\right)\overline{S}_i(a)\ .
\end{aligned}$$

6.5 Building infinite families of extension degrees

In the previous section, we set an extension degree m and studied the corresponding exponents s dividing 2^m+1. It is however customary to go the other way around, i.e. set an exponent s, or a given form of exponents, which is valid for an infinite family of extension degrees m and devise characterizations valid for this infinity of extension degrees. In this section, we provide the link between these two approaches.

More precisely, we supposed above that the additional trace term had a Dillon-like exponent, i.e. that is was of the form $s(2^m-1)$ where s divides 2^m+1 and $\tau=\frac{2^m+1}{s}$. Hence, the Dillon-like exponent could be written as $\frac{2^n-1}{\tau}=\frac{2^m+1}{\tau}(2^m-1)$ and the above construction then relied on the fact that τ divided 2^m+1, that is that $2^m\equiv -1 \pmod{\tau}$ or equivalently that -1 was in the cyclotomic coset of 1 modulo 2^m+1.

The problem we tackle in this section is the following: fix a value for τ and devise the extension degrees m for which τ divides 2^m+1. In fact, there are only two possibilities for a given τ: either there is an infinity of such extension degrees, or there is no extension degree at all. Therefore, we focus on the construction and characterization of values of τ for which an infinite number of such extension degrees m exists, starting with prime numbers and then extending our approach to prime powers and finally to odd composite numbers. The number 2^m+1 is obviously odd so that an even τ can not divide 2^m+1 and this last case covers all possibilities for τ.

6.5.1 Prime case

Let p be an odd prime number and set $\tau=p$. The set of modular integers $\mathbb{Z}/p\mathbb{Z}$ is a field and there exists i such that $2^i\equiv -1 \pmod{p}$ if and only if the multiplicative order of 2 modulo p is even. In this case, $2^m\equiv -1 \pmod{p}$ if and only if $m\equiv o \pmod{2o}$, where $2o$ is the multiplicative order of 2 modulo p. In particular, the family of such extension degrees m is infinite. The size $t=o(s)$ of the cyclotomic coset of $s=(2^m+1)/p$ modulo 2^m+1 is then

$$t=2o\ .$$

Furthermore, one has

$$2^m \equiv 2^o \pmod{2^t - 1} \ ,$$

so that if $f_{a,b} \in \mathcal{H}_n$ is hyper-bent, then its dual is $f_{a,b^{2^o}}$.

To actually devise such prime numbers, we now focus on the specific case where the multiplicative order of 2 modulo p is maximal, that is where 2 is a primitive root modulo p. In this situation, the above condition becomes

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p} \ .$$

This implies that the Legendre symbol $\left(\frac{2}{p}\right)$ of 2 modulo p is -1 and that 2 is a quadratic nonresidue modulo p. It is well-known that the Legendre symbol of 2 modulo an odd prime p is

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \ , \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \ . \end{cases}$$

Therefore, if 2 is a primitive root modulo p, then one must have $p \equiv \pm 3 \pmod 8$. This gives a practical criterion to discard prime numbers such that 2 is not a primitive element. Further characterizations of primes p such that 2 is a primitive root modulo p can be found in a paper of Park, Park and Kim [217].

For such a prime number p, $2^m \equiv -1 \pmod p$ if and only if $m \equiv \frac{p-1}{2} \pmod{p-1}$. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m + 1)/p$ modulo $2^m + 1$ is then

$$t = p - 1 \ .$$

Finding an infinite number of odd prime numbers for which 2 is a primitive element would thus give an elegant solution to our problem, i.e. finding an infinite family of denominators $\tau = p$ associated with infinite families of extension degrees m. This question is however difficult; it is a special case of Artin's conjecture on primitive roots.

Conjecture 6.5.1 (Artin's conjecture on primitive roots)**.** *Let a be an integer which is neither a perfect square nor -1. Then the number of primes numbers p such that a is a primitive element modulo p is infinite.*

It should be noted that Artin's conjecture has been proved by Hooley [129] under the Generalized Riemann Hypothesis. Heath-Brown [123] has proved unconditionally that there exist at most two exceptional primes for which Artin's conjecture fails; nonetheless, this proof is non-constructive.

From a more computational perspective, the first elements of the sequence of primes such that 2 is a primitive element is sequence `A001122` in OEIS [136] and begins with

$$3,\ 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ 53,\ 59,\ 61,\ 67,\ 83 \ .$$

As mentioned in the beginning of this section, it is not necessary that 2 is a primitive root modulo 2 for 1 and -1 to lie in the same cyclotomic coset modulo p. The list of odd primes p smaller than 100 such that the multiplicative order of 2 modulo p is even and a strict divisor of $p-1$, together with half the order o of 2, i.e. the smallest integer o such that $2^o \equiv -1 \pmod p$, is

$$(17, 4),\ (41, 10),\ (43, 7),\ (97, 24) \ .$$

Finally, there exist as well odd primes for which 1 and -1 are not in the same cyclotomic coset modulo p. The list of such primes smaller than 100 is

$$7,\ 23,\ 31,\ 47,\ 71,\ 73,\ 79,\ 89 \ .$$

6.5.2 Prime power case

Let p be an odd prime number and $k \geq 2$ a positive integer. Set $\tau = p^k$. The multiplicative group of units modulo p^k is once again cyclic and isomorphic to

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^{k-1} \quad .$$

The condition for the prime case is thus still valid; there exists i such that $2^i \equiv -1 \pmod{p^k}$ if and only if the multiplicative order of 2 modulo p^k is even. In this case, $2^m \equiv -1 \pmod{p^k}$ if and only if $m \equiv o \pmod{2o}$, where $2o$ is the multiplicative order of 2 modulo p^k. In particular, the family of such extension degrees is also infinite. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m + 1)/p^k$ modulo $2^m + 1$, is then

$$t = 2o \ .$$

If $f_{a,b} \in \mathcal{H}_n$ is hyper-bent, then its dual is $f_{a,b^{2^o}}$.

It is a classical result [70, Lemma 1.4.5 and following remarks], that if an integer a is a primitive root modulo p, then a or $a + p$ is a primitive root modulo p^2. Furthermore, if a is a primitive root modulo p^2, then it is modulo p^k for any $k \geq 2$ [70, Lemma 1.4.5 and following remarks]. Conversely, if a is not a primitive root modulo p^i, then it is not a primitive root modulo p^k for any $k \geq i$. The approach of the previous subsection can therefore be extended to any prime power p^k with $k \geq 2$ by just checking that 2 is a primitive root modulo p^2. If it is, then

$$2^{\frac{\phi(p^k)}{2}} \equiv -1 \pmod{\phi(p^k)}$$

for any $k \geq 2$, where ϕ denotes Euler's totient function. In particular, we have $\phi(p^k) = (p-1)p^{k-1}$. In this case, one would choose $m \equiv \frac{\phi(p^k)}{2} \pmod{\phi(p^k)}$. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m + 1)/p^k$ modulo $2^m + 1$, is then

$$t = \phi(p^k) \ .$$

The primes smaller than 100 such that 2 is a primitive root modulo p^2 are

$$3,\ 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ 53,\ 59,\ 61,\ 67,\ 83 \ .$$

From a computational perspective, more can be said. Indeed, if 2 is a primitive root modulo p, but is not modulo p^2, a simple calculation shows that $2^{p-1} \equiv 1 \pmod{p^2}$, that is p is a *Wieferich prime*. The sequence of such primes is sequence `A001220` in the OEIS [136]. Only two of them are currently known: 1093 and 3511; and 2 is not a primitive root for both of these primes. Checking that 2 is a primitive root modulo p is therefore enough to ensure that it is modulo any power of p as long as p is not too large, less than fifteen decimal digits according to Dorais and Klyve [95].

The list of odd primes p smaller than 100 such that the multiplicative order of 2 modulo p^2 is even and a strict divisor of $\phi(p^2)$, together with half the order o of 2, i.e. the smallest integer o such that $2^o \equiv -1 \pmod{p^2}$, is

$$(17, 68),\ (41, 410),\ (43, 301),\ (97, 2328) \ .$$

Finally, the list of odd primes p smaller than 100 such that 1 and -1 do not lie in the same cyclotomic coset modulo p^2 is

$$7,\ 23,\ 31,\ 47,\ 71,\ 73,\ 79,\ 89 \ .$$

6.5.3 Composite case

We now consider the general case of an odd composite number. Suppose that $\tau = p_1^{k_1} \cdots p_r^{k_r}$ is a product of $r \geq 2$ distinct prime powers.

The multiplicative group of units modulo τ is not cyclic anymore and is isomorphic to the product of the cyclic groups corresponding to each prime power:

$$(\mathbb{Z}/\tau\mathbb{Z})^\times \simeq \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{k_r}\mathbb{Z}\right)^\times \ .$$

The multiplicative order of 2 modulo τ is the least common multiple of its multiplicative orders modulo the prime powers dividing τ. There exists an integer i such that $2^i \equiv -1 \pmod{\tau}$ if and only if there exists such integers for each prime power dividing τ, that is if the multiplicative order of 2 modulo $p_j^{k_j}$ is even for $1 \leq j \leq r$, and if moreover their least common multiple is an odd multiple of each of them, that is if they all have the same 2-adic valuation. In such a situation, $2^m \equiv -1 \pmod{\tau}$ if and only if $m \equiv o \pmod{2o}$, where $2o$ is the multiplicative order of 2 modulo τ. In particular, the family of such extension degrees is still infinite. Recall that the corresponding denominator is τ. The size $t = o(s)$ of the cyclotomic coset of $s = (2^m + 1)/\tau$ modulo $2^m + 1$, is then

$$t = 2o \ .$$

If $f_{a,b} \in \mathcal{H}_n$ is hyper-bent, then its dual is $f_{a,b^{2^o}}$.

In particular, if 2 is a primitive root modulo each prime power dividing τ, then the multiplicative order of 2 modulo τ is

$$2o = \mathrm{lcm}(\phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r})) \ ,$$

and $2^o \equiv -1 \pmod{\tau}$ if and only if $\nu_2(p_1 - 1) = \cdots = \nu_2(p_r - 1)$, where ν_2 denotes the 2-adic valuation. Conditioned by the fact that there exists an infinite number of primes p such that 2 is a primitive root modulo p or modulo p^2 and such that $p - 1$ has a given 2-adic valuation, we can construct an infinite number of composite odd numbers addressing our original problem.

The list of suitable odd composite numbers τ smaller than 100, together with half the multiplicative order o of 2 modulo τ, that is the smallest integer such that $2^o \equiv -1 \pmod{\tau}$, is

$$(33, 5), \ (57, 9), \ (65, 6), \ (99, 15) \ .$$

6.6 Applications

In this section, we show how the results of Section 6.4 can be applied to several infinite families of Boolean functions in order to obtain characterizations of their hyper-bentness in terms of exponential sums over $\mathcal{T}_1 \subset \mathbb{F}_{2^m}$. Such characterizations can easily be transformed into characterizations involving complete exponential sums over $\mathbb{F}_{2^m}$ using Lemma 2.4.8, or the Hamming weights of g_a and the related function $x \mapsto \mathrm{Tr}_1^m(1/x) + g_a(x)$ defined over $\mathbb{F}_{2^m}$. Much of these applications can be straightforwardly extended to additional cases.

6.6.1 The case $b = 1$

We first apply results of Subsections 6.4.1 and 6.4.2 to $f_{a,1}$ defined as in Equation (6.8) in the specific case where $b = 1$.

Since 1 lies in $\mathbb{F}_2$, there exists $\beta \in \mathbb{F}_{2^m} \subset \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_t^n(\beta) = 1$. In particular, $f_{a,1}$ belongs to both families $\mathcal{G}_n$ and $\mathcal{H}_n$. In fact, the discussion in Section 6.5, shows that $m \equiv o \pmod{2o}$ and that $t = o(s) = 2o$ where $2o$ is the multiplicative order of 2 modulo $\tau = \frac{2^m+1}{s}$.

Hence, $n/t = m/l$ is odd and β can be chosen to be 1. Applying Theorem 6.4.9 shows that $f_{a,1}$ is hyper-bent if and only if

$$\sum_{t\in\mathcal{T}_1} \chi\left(\sum_{r\in R} \mathrm{Tr}_1^m\left(a_r D_r(t)\right) + \mathrm{Tr}_1^m\left(D_s(t)\right)\right) = 0 \ .$$

Applying Lemma 2.4.8, this condition is straightforwardly expressed in terms of complete exponential sums over $\mathbb{F}_{2^m}$, or of the Hamming weights of $g'_a : x \mapsto g_a(x) + \mathrm{Tr}_1^m\left(D_s(t)\right)$ and the related function $x \mapsto \mathrm{Tr}_1^m\left(1/x\right) + g'_a(x)$ defined over $\mathbb{F}_{2^m}$. To summarize, we have the following characterization for the value of $\Lambda(a,1)$ and so for the hyper-bentness for $f_{a,1}$.

Proposition 6.6.1. *Let g'_a be the Boolean function defined on $\mathbb{F}_{2^m}$ as $g'_a(x) = g_a(x)+\mathrm{Tr}_1^m\left(D_s(x)\right)$. Then*

$$\Lambda(a,1) = 2T_1(g'_a) + 1 \ .$$

In particular, $f_{a,1}$ is hyper-bent if and only if

$$T_1(g'_a) = 0 \ .$$

We now show how the results of Subsection 6.4.2 can be applied to obtain a different characterization of the hyper-bentness of $f_{a,1}$. According to Proposition 6.4.2, $f_{a,1}$ is hyper-bent if and only if

$$\Lambda(a,1) = 1 \ .$$

Let ξ be a primitive τ-th root of unity. First, recall that ξ lies in $\mathbb{F}_{2^t}$, that $\mathrm{Tr}_1^t\left(\xi^2\right) = \mathrm{Tr}_1^t\left(\xi\right)$ and that

$$\sum_{i=0}^{\tau-1} \xi^i = 0 \ .$$

Second, remark that the results of Section 6.5 imply that t is even, so that $\mathrm{Tr}_1^t\left(1\right) = 0$. Moreover, ξ is a $(2^{t/2}+1)$-th root of unity so that $\xi + \xi^{-1} \in \mathbb{F}_{2^{t/2}}$ which implies that

$$\mathrm{Tr}_1^t\left(\xi^i\right) = \mathrm{Tr}_1^t\left(\xi^{-i}\right) \ .$$

Finally, Proposition 6.4.20 reads

$$\Lambda(a,1) = \overline{S}_0(a) + 2\sum_{i=1}^{\frac{\tau-1}{2}} \chi\left(\mathrm{Tr}_1^t\left(\xi^i\right)\right)\overline{S}_i(a) \ .$$

Nonetheless, the trace of ξ^i for $i \neq 0$ depends on the exact value of τ. In the sequel, we deal with some specific cases.

Prime case

For simplicity, we first suppose that $\tau = p$ is a prime and that 2 is a primitive root modulo p. In this case, we have $t = p-1$ and i is co-prime with p, so that

$$\mathrm{Tr}_1^{p-1}\left(\xi^i\right) = \sum_{j=0}^{p-2} \xi^{i2^j} = \sum_{j=1}^{p-1} \xi^{ij} = \sum_{j=1}^{p-1} \xi^j = 1 \ .$$

Therefore

$$\Lambda(a,1) = 2\overline{S}_0(a) - \sum_{i=0}^{p-1} \overline{S}_i(a) \ .$$

Applying Lemma 6.4.21 with $l = 1$ and $l = p$ yields

$$\Lambda(a,1) = \frac{2}{p}(1 + 2T_1(g_a \circ D_p)) - (1 + 2T_1(g_a)) \ .$$

Consequently, we get the following characterization.

Proposition 6.6.2. *Suppose that $\tau = p$ is a prime and that 2 is a primitive root modulo p. Then*

$$p\Lambda(a,1) = 4T_1(g_a \circ D_p) - 2pT_1(g_a) - p + 2 \ .$$

In particular, $f_{a,1}$ is hyper-bent if and only if

$$2T_1(g_a \circ D_p) - pT_1(g_a) = p - 1 \ .$$

Prime power case

We now treat the case where $\tau = p^k$ is a prime power and that 2 is a primitive root modulo p^k, including the prime case where $k = 1$. Then $t = \phi(p^k) = (p-1)p^{k-1}$. Remark that in this situation, for every positive integers $i \geq 0$ and $j > 0$ such that $i+j = k$, one has $\left(\xi^{p^i}\right)^{p^j} = \xi^{p^k} = 1$, so that

$$\sum_{l=0}^{p^j-1} \xi^{lp^i} = 0 \ . \tag{6.9}$$

Then

$$\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) = \sum_{j=0}^{\phi(p^k)-1} \xi^{i2^j} = \sum_{1 \leq j \leq p^k-1,\ p \nmid j} \xi^{ij} \ .$$

If $p^e \,||\, i$ with $0 \leq e \leq k-1$, then $i = lp^e$ with l co-prime with $p-1$ and

$$\begin{aligned}
\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) &= \sum_{1 \leq j \leq p^k-1,\ p \nmid j} \xi^{jlp^e} \\
&= \sum_{1 \leq j \leq p^k-1,\ p \nmid j} \xi^{jp^e} \\
&= \sum_{j=0}^{p^k-1} \xi^{jp^e} + \sum_{j=0}^{p^{k-1}-1} \xi^{jp^{e+1}} \\
&= \sum_{j=0}^{p^k-1} \xi^{jp^e} + \sum_{j=0}^{p^k-1} \xi^{jp^{e+1}} + \sum_{j=p^{k-1}}^{p^k-1} \xi^{jp^{e+1}} \ .
\end{aligned}$$

Equation (6.9) shows that the first two sums of the right hand side of the last equality can be split into a multiple of sums equal to zero. If $0 \leq e \leq k-2$, then the third sum is zero as well, so that

$$\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) = 0 \ .$$

If $e = k-1$, then the third sum reads

$$\sum_{j=p^{k-1}}^{p^k-1} \xi^{jp^k} = \sum_{j=p^{k-1}}^{p^k-1} \xi^j = 1 \ .$$

Therefore

$$\mathrm{Tr}_1^{\phi(p^k)}\left(\xi^i\right) = 1 \ .$$

Summing up the above observations yields

$$\begin{aligned}\Lambda(a,1) &= \sum_{i=0}^{p^k-1} \overline{S}_i(a) - 2\sum_{i=1}^{p-1} \overline{S}_{ip^{k-1}}(a) \\ &= 2\overline{S}_0(a) + \sum_{i=0}^{p^k-1} \overline{S}_i(a) - 2\sum_{i=0}^{p-1} \overline{S}_{ip^{k-1}}(a) \ .\end{aligned}$$

Applying Lemma 6.4.21 with $l = 1$, $l = p^{k-1}$ and $l = p^k$ then gives

$$\Lambda(a,1) = \frac{2}{p^k}(1 + 2T_1(g_a \circ D_{p^k})) - \frac{2}{p^{k-1}}(1 + 2T_1(g_a \circ D_{p^{k-1}})) + (1 + 2T_1(g_a)) \ .$$

Consequently, we get the following characterization.

Proposition 6.6.3. *Suppose that $\tau = p^k$ is a prime power and that 2 is a primitive root modulo p^k. Then*

$$p^k\Lambda(a,1) = 4T_1(g_a \circ D_{p^k}) - 4pT_1(g_a \circ D_{p^{k-1}}) + 2p^kT_1(g_a) + p^k - 2p + 2 \ .$$

In particular, $f_{a,1}$ is hyper-bent if and only if

$$2T_1(g_a \circ D_{p^k}) - 2pT_1(g_a \circ D_{p^{k-1}}) + p^kT_1(g_a) = p - 1 \ .$$

6.6.2 Explicit values for τ

The previous subsection dealt with a fixed value of $b \in \mathbb{F}_{2^t}^*$ casting as few restrictions as possible on τ. In this subsection we go the other way around and treat the first few possible values of τ for all values of b with as few restrictions as possible on the corresponding infinite family of Boolean functions. Hence, we consider functions $f_{a,b} \in \mathcal{H}_n$ of the form

$$f_{a,b}(x) = \sum_{r \in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^t\left(bx^{\frac{2^m+1}{\tau}(2^m-1)}\right)$$

for a fixed value of τ as in Equation (6.8). Recall that such functions are hyper-bent if and only if the associated exponential sum $\Lambda(a,b) = \Lambda(f_{a,b})$ is equal to 1. Thus, the explicit expressions for $\Lambda(a,b)$ that we give in this subsection trivially turn into characterizations for hyper-bentness of $f_{a,b}$.

A large part of the data presented in this subsection has been checked or generated with the mathematical software Sage [241]. In addition to the functionality provided by Sage itself, the computations involved used, for the most, the underlying libraries Givaro [96] for finite field arithmetic, and Pynac [250] for symbolic manipulations. For small values of τ, that is $\tau = 3$, 5 and 9, we provide all details and corresponding data. For higher values of τ, only the characterizations we obtain are given. The basic algorithm used is an explicit version of the approach taken in the previous subsection. To find characterizations valid for

- an integer τ such that 1 and -1 lie in the same cyclotomic class modulo τ,
- a coefficient $b \in \mathbb{F}_{2^{2o}}^*$ where $2o$ is the multiplicative order of 2 modulo τ,
- a divisor l of o,
- an l-th root r of -1 modulo τ and corresponding extension degrees m,
- and coefficients $a_r \in \mathbb{F}_{2^{\frac{m}{l}}}$,

we proceed as described in Algorithm 6.1.

Algorithm 6.1: Expression for $\Lambda(a,b)$ in terms of the sums $T_1(g_a \circ D_k)$

Input: An integer τ and associated data.
Output: Expression for $\Lambda(a,b)$ in terms of the sums $T_1(g_a \circ D_k)$

1 Compute the traces $\mathrm{Tr}_1^{2o}\left(b\xi^i\right)$, where ξ is a primitive element of $\mathbb{F}_{2^{2o}}$
2 Deduce an expression of $\Lambda(a,b)$ in terms of the sums S_i using Proposition 6.4.20
3 Compute the orbits of invertible integers modulo τ under the action of multiplication by r
4 Devise relations between the sums S_i using Lemma 6.4.23
5 Express the sums S_i in terms of the sums $T_1(g_a \circ D_k)$, where k divides τ, using Lemma 6.4.21
6 If possible, deduce an expression of $\Lambda(a,b)$ in terms of the sums $T_1(g_a \circ D_k)$

The case $\tau = 3$

The smallest possible value for τ is $\tau = 3$. This case was originally addressed by the author in 2009 for the binomial case [197] and further in 2010 for the general case [192]. We now show how the characterizations for the general case can be directly deduced from the results of Section 6.4.

In this case, we have $t = 2$ and $m \equiv 1 \pmod 2$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is f_{a,b^2}.

According to Remark 6.4.24, we have

$$\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^2(b)\right)\overline{S}_0(a) + \left(\chi\left(\mathrm{Tr}_1^2(b\xi)\right) + \chi\left(\mathrm{Tr}_1^2\left(b\xi^{-1}\right)\right)\right)\overline{S}_1(a) \ .$$

Note that ξ is a primitive 3-rd root of unity and that $\xi + \xi^{-1} = 1$, so that

$$\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^2(b)\right)\overline{S}_0(a) + \chi\left(\mathrm{Tr}_1^2(b\xi)\right)\left(1 + \chi\left(\mathrm{Tr}_1^2(b)\right)\right)\overline{S}_1(a) \ .$$

Moreover, we have $\mathbb{F}_4^* = \langle\xi\rangle$. Thus, if $b = 1$, then $\Lambda(a,1) = \overline{S}_0(a) - 2\overline{S}_1(a)$, and if $b = \xi$ or $b = \xi^{-1}$, that is if b is a primitive 3-rd root of unity or equivalently a primitive element of $\mathbb{F}_4$, then $\Lambda(a,b) = -\overline{S}_0(a)$. Applying Lemma 6.4.21 with $l = 1$ and $l = 3$ then gives the following theorem and the corresponding characterizations for hyper-bentness.

Theorem 6.4.4 ([192]). *Let $\tau = 3$ and $m \equiv 1 \pmod 2$. Then*

1. *If $b = 1$, then $3\Lambda(a,1) = 4T_1(g_a \circ D_3) - 6T_1(g_a) - 1$.*
2. *If b is a primitive element of $\mathbb{F}_4$, then $3\Lambda(a,b) = -2T_1(g_a \circ D_3) - 1$.*

Table 6.3 – Traces $\mathrm{Tr}_1^4\left(\beta^j\xi^i\right)$ for $\tau = 5$

$j\backslash i$	0	1	2	3	4
0	0	1	1	1	1
1	0	0	1	0	1
2	0	0	0	1	1
3	1	1	1	1	0
4	0	1	0	1	0
5	0	0	1	1	0
6	1	1	1	0	1
7	1	0	1	0	0

$j\backslash i$	0	1	2	3	4
8	0	1	1	0	0
9	1	1	0	1	1
10	0	1	0	0	1
11	1	1	0	0	0
12	1	0	1	1	1
13	1	0	0	1	0
14	1	0	0	0	1

The case $\tau = 5$

The next possible value for τ is $\tau = 5$. This case was originally addressed by Wang et al. in late 2011 for the general case [258], but they also gave specific treatments for the binomial case [257, 256]. We now show how their characterizations for the general case can be directly deduced from the results of Section 6.4.

In this case, we have $t = 4$ and $m \equiv 2 \pmod 4$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is f_{a,b^4}.

According to Remark 6.4.24, we have

$$\begin{aligned}\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^4(b)\right)\overline{S}_0(a) \\ + \left(\chi\left(\mathrm{Tr}_1^4(b\xi)\right) + \chi\left(\mathrm{Tr}_1^4\left(b\xi^{-1}\right)\right)\right)\overline{S}_1(a) \\ + \left(\chi\left(\mathrm{Tr}_1^4\left(b\xi^2\right)\right) + \chi\left(\mathrm{Tr}_1^4\left(b\xi^{-2}\right)\right)\right)\overline{S}_2(a) \ .\end{aligned}$$

Introduce $\gamma = \xi + \xi^{-1} \in \mathbb{F}_4$. Then

$$\begin{aligned}\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^4(b)\right)\overline{S}_0(a) \\ + \chi\left(\mathrm{Tr}_1^4(b\xi)\right)\left(1 + \chi\left(\mathrm{Tr}_1^4(b\gamma)\right)\right)\overline{S}_1(a) \\ + \chi\left(\mathrm{Tr}_1^4\left(b\xi^2\right)\right)\left(1 + \chi\left(\mathrm{Tr}_1^4\left(b\gamma^2\right)\right)\right)\overline{S}_2(a) \ .\end{aligned}$$

Next, recall that ξ is a 5-th root of unity, so that $\sum_{i=0}^4 \xi^i = 0$. In particular, we have $\gamma + \gamma^2 = 1$ and

$$\mathrm{Tr}_1^4(b\gamma) + \mathrm{Tr}_1^4\left(b\gamma^2\right) = \mathrm{Tr}_1^4(b) \ ,$$

what can be used to refine the above expression.

Here, we rather explicitly compute all the traces $\mathrm{Tr}_1^4\left(b\xi^i\right)$. The finite field $\mathbb{F}_{16}$ is represented as $\mathbb{F}_2[x]/(C_4(x))$ where $C_4(x) = x^4 + x + 1$ is the 4-th Conway polynomial. We denote the class of x modulo $C_4(x)$ by β; this is a primitive element of $\mathbb{F}_{16}$. Let $\xi = \beta^3$ be a 5-th root of unity. The traces $\mathrm{Tr}_1^4\left(\beta^j\xi^i\right)$ are given in Table 6.3. The expression of $\Lambda(a,\beta^j)$ as a sum of the partial exponential sums $\overline{S}_i$, together with the minimal polynomial m_j of β^j, are given in Table 6.4.

Moreover, if the coefficients a_r lie in $\mathbb{F}_{2^l}$, where $l = m/2$, then $l \equiv 1 \pmod 2$ and $2^l \equiv \pm 2 \pmod 5$. Lemma 6.4.23 tells that either $\overline{S}_1(a) = \overline{S}_2(a)$ or $\overline{S}_1(a) = \overline{S}_3(a)$. But $\overline{S}_2(a) = \overline{S}_3(a)$, so that one always has

$$\overline{S}_1(a) = \overline{S}_2(a) \ .$$

Finally applying Lemma 6.4.21 for $l = 1$ and $l = 5$ gives the following theorem which summarizes the above discussion.

Table 6.4 – $\Lambda(a, \beta^j)$ for $\tau = 5$

j	$\Lambda(a, \beta^j)$	m_j
0	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2$	$x+1$
1	$\overline{S}_0$	x^4+x+1
2	$\overline{S}_0$	x^4+x+1
3	$-\overline{S}_0 - 2\overline{S}_2$	$x^4+x^3+x^2+x+1$
4	$\overline{S}_0$	x^4+x+1
5	$\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2$	x^2+x+1
6	$-\overline{S}_0 - 2\overline{S}_1$	$x^4+x^3+x^2+x+1$
7	$-\overline{S}_0 + 2\overline{S}_1$	x^4+x^3+1
8	$\overline{S}_0$	x^4+x+1
9	$-\overline{S}_0 - 2\overline{S}_1$	$x^4+x^3+x^2+x+1$
10	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2$	x^2+x+1
11	$-\overline{S}_0 + 2\overline{S}_2$	x^4+x^3+1
12	$-\overline{S}_0 - 2\overline{S}_2$	$x^4+x^3+x^2+x+1$
13	$-\overline{S}_0 + 2\overline{S}_1$	x^4+x^3+1
14	$-\overline{S}_0 + 2\overline{S}_2$	x^4+x^3+1

Theorem 6.6.5 ([258]). *Let $\tau = 5$ and $m \equiv 2 \pmod 4$.*

1. *If $b = 1$, then $5\Lambda(a,b) = 4T_1(g_a \circ D_5) - 10T_1(g_a) - 3$.*
2. *If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, i.e. with minimal polynomial x^4+x+1, then $5\Lambda(a,b) = 2T_1(g_a \circ D_5) + 1$.*
3. *Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$.*
   (a) *If b is a primitive 3-rd root of unity, i.e. with minimal polynomial x^2+x+1, then $5\Lambda(a,b) = 2T_1(g_a \circ D_5) + 1$.*
   (b) *If b is a primitive 5-th root of unity, i.e. with minimal polynomial $x^4+x^3+x^2+x+1$, then $5\Lambda(a,b) = -T_1(g_a \circ D_5) - 5T_1(g_a) - 3$.*
   (c) *If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 1$, i.e. with minimal polynomial x^4+x^3+1, then $5\Lambda(a,b) = -3T_1(g_a \circ D_5) + 5T_1(g_a) + 1$.*

The case $\tau = 7$

For $\tau = 7$, 1 and -1 do not lie in the same cyclotomic coset modulo 7, hence the next suitable value for τ is $\tau = 9$.

The case $\tau = 9$

In the case $\tau = 9$, we have $t = 6$ and $m \equiv 3 \pmod 6$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is f_{a,b^8}.

According to Remark 6.4.24, we have

$$\begin{aligned}\Lambda(a,b) = {} & \chi\left(\mathrm{Tr}_1^6(b)\right)\overline{S}_0(a) \\ & + \left(\chi\left(\mathrm{Tr}_1^6(b\xi)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^8)\right)\right)\overline{S}_1(a) + \left(\chi\left(\mathrm{Tr}_1^6(b\xi^2)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^7)\right)\right)\overline{S}_2(a) \\ & + \left(\chi\left(\mathrm{Tr}_1^6(b\xi^3)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^6)\right)\right)\overline{S}_3(a) + \left(\chi\left(\mathrm{Tr}_1^6(b\xi^4)\right) + \chi\left(\mathrm{Tr}_1^6(b\xi^5)\right)\right)\overline{S}_4(a) \ .\end{aligned}$$

Introduce $\gamma = \xi^8 + \xi \in \mathbb{F}_8$. Note that we have

$$\begin{aligned}
\gamma^2 &= \xi^2 + \xi^7 \ , \\
\gamma^3 &= \xi + \xi^3 + \xi^6 + \xi^8 \ , \\
\gamma^4 &= \xi^4 + \xi^5 \ , \\
\gamma^5 &= \xi^3 + \xi^4 + \xi^5 + \xi^6 \ , \\
\gamma^6 &= \xi^2 + \xi^3 + \xi^6 + \xi^7 \ .
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\Lambda(a,b) = \chi\left(\mathrm{Tr}_1^6(b)\right)\overline{S}_0(a) \\
&+ \chi\left(\mathrm{Tr}_1^6(b\xi)\right)\left(1+\chi\left(\mathrm{Tr}_1^6(b\gamma)\right)\right)\overline{S}_1(a) \\
&+ \chi\left(\mathrm{Tr}_1^6\left(b\xi^2\right)\right)\left(1+\chi\left(\mathrm{Tr}_1^6\left(b\gamma^2\right)\right)\right)\overline{S}_2(a) \\
&+ \chi\left(\mathrm{Tr}_1^6\left(b\xi^3\right)\right)\left(1+\chi\left(\mathrm{Tr}_1^6\left(b(\gamma^3+\gamma)\right)\right)\right)\overline{S}_3(a) \\
&+ \chi\left(\mathrm{Tr}_1^6\left(b\xi^4\right)\right)\left(1+\chi\left(\mathrm{Tr}_1^6\left(b\gamma^4\right)\right)\right)\overline{S}_4(a) \ .
\end{aligned}$$

Next, recall that $\sum_{i=0}^{8}\xi^i = 0$. Hence, we have $\gamma^2+\gamma^3+\gamma^4 = 1$ and

$$\mathrm{Tr}_1^6(b\gamma) + \mathrm{Tr}_1^6\left(b\gamma^2\right) + \mathrm{Tr}_1^6\left(b(\gamma+\gamma^3)\right) + \mathrm{Tr}_1^6\left(b\gamma^4\right) = \mathrm{Tr}_1^6(b) \ ,$$

what can be used to refine the above expression for $\Lambda(a,b)$.

Here, we rather explicitly compute all the traces $\mathrm{Tr}_1^6\left(b\xi^i\right)$. The finite field $\mathbb{F}_{64}$ is represented as $\mathbb{F}_2[x]/(C_6(x))$ where $C_6(x) = x^6+x^4+x^3+x+1$ is the 6-th Conway polynomial. We denote the class of x modulo $C_6(x)$ by β; this is a primitive element of $\mathbb{F}_{64}$. Let $\xi = \beta^7$ be a 9-th root of unity. The traces $\mathrm{Tr}_1^6\left(\beta^j\xi^i\right)$ are given in Table 6.5. The expression of $\Lambda(a,\beta^j)$ as a sum of the partial exponential sums $\overline{S}_i$, together with the minimal polynomial m_j of β^j, are given in Tables 6.6 and 6.7.

Moreover, if the coefficients a_r lie in $\mathbb{F}_{2^l}$, where $l = m/3$, then 2^l is -1, 2 or -4 modulo 9 when l is respectively 0, 1 and 2 modulo 3. In the last two cases, Lemma 6.4.23 tells that

$$\overline{S}_1(a) = \overline{S}_2(a) = \overline{S}_4(a) \ .$$

The corresponding expressions for $\Lambda(a,b)$, obtained after applying Lemma 6.4.21 for $l=1$, $l=3$ and $l=9$, are given in Table 6.8, where m_b is the minimal polynomial of b.

Finally, the following theorem summarizes the above discussion.

Theorem 6.6.6. *Let $\tau = 9$ and $m \equiv 3 \pmod 6$.*

1. *If $b = 1$, then*

$$9\Lambda(a,b) = 4T_1(g_a \circ D_9) - 12T_1(g_a \circ D_3) + 18T_1(g_a) + 5 \ .$$

2. *If b is a primitive 3-rd root of unity, then*

$$9\Lambda(a,b) = -2T_1(g_a \circ D_9) - 6T_1(g_a \circ D_3) + 18T_1(g_a) + 5 \ .$$

3. *Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{3}}}$ and $\frac{m}{3} \not\equiv 0 \pmod 3$.*

Table 6.5 – Traces $\mathrm{Tr}_1^6\left(\beta^j\xi^i\right)$ for $\tau = 9$

$j\backslash i$	0	1	2	3	4	5	6	7	8
0	0	0	0	1	0	0	1	0	0
1	0	0	0	1	1	0	1	1	0
2	0	0	0	1	0	1	1	0	1
3	1	0	0	1	1	1	0	1	1
4	0	1	0	1	0	0	1	1	0
5	0	1	1	1	1	0	1	0	1
6	1	1	0	0	0	1	1	1	1
7	0	0	1	0	0	1	0	0	0
8	0	0	1	1	0	1	1	0	0
9	0	0	1	0	1	1	0	1	0
10	0	0	1	1	1	0	1	1	1
11	1	0	1	0	0	1	1	0	0
12	1	1	1	1	0	1	0	1	0
13	1	0	0	0	1	1	1	1	1
14	0	1	0	0	1	0	0	0	0
15	0	1	1	0	1	1	0	0	0
16	0	1	0	1	1	0	1	0	0
17	0	1	1	1	0	1	1	1	0
18	0	1	0	0	1	1	0	0	1
19	1	1	1	0	1	0	1	0	1
20	0	0	0	1	1	1	1	1	1
21	1	0	0	1	0	0	0	0	0
22	1	1	0	1	1	0	0	0	0
23	1	0	1	1	0	1	0	0	0
24	1	1	1	0	1	1	1	0	0
25	1	0	0	1	1	0	0	1	0
26	1	1	0	1	0	1	0	1	1
27	0	0	1	1	1	1	1	1	0
28	0	0	1	0	0	0	0	0	1
29	1	0	1	1	0	0	0	0	1
30	0	1	1	0	1	0	0	0	1
31	1	1	0	1	1	1	0	0	1

$j\backslash i$	0	1	2	3	4	5	6	7	8
32	0	0	1	1	0	0	1	0	1
33	1	0	1	0	1	0	1	1	1
34	0	1	1	1	1	1	1	0	0
35	0	1	0	0	0	0	0	1	0
36	0	1	1	0	0	0	0	1	1
37	1	1	0	1	0	0	0	1	0
38	1	0	1	1	1	0	0	1	1
39	0	1	1	0	0	1	0	1	0
40	0	1	0	1	0	1	1	1	1
41	1	1	1	1	1	1	0	0	0
42	1	0	0	0	0	0	1	0	0
43	1	1	0	0	0	0	1	1	0
44	1	0	1	0	0	0	1	0	1
45	0	1	1	1	0	0	1	1	1
46	1	1	0	0	1	0	1	0	0
47	1	0	1	0	1	1	1	1	0
48	1	1	1	1	1	0	0	0	1
49	0	0	0	0	0	1	0	0	1
50	1	0	0	0	0	1	1	0	1
51	0	1	0	0	0	1	0	1	1
52	1	1	1	0	0	1	1	1	0
53	1	0	0	1	0	1	0	0	1
54	0	1	0	1	1	1	1	0	1
55	1	1	1	1	0	0	0	1	1
56	0	0	0	0	1	0	0	1	0
57	0	0	0	0	1	1	0	1	1
58	1	0	0	0	1	0	1	1	0
59	1	1	0	0	1	1	1	0	1
60	0	0	1	0	1	0	0	1	1
61	1	0	1	1	1	1	0	1	0
62	1	1	1	0	0	0	1	1	1

Table 6.6 – $\Lambda(a, \beta^j)$ for $\tau = 9$ — Part I

j	$\Lambda(a, \beta^j)$	m_j
0	$\overline{S}_0 + 2\overline{S}_1 + 2\overline{S}_2 - 2\overline{S}_3 + 2\overline{S}_4$	$x+1$
1	$\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_3$	$x^6+x^4+x^3+x+1$
2	$\overline{S}_0 + 2\overline{S}_2 - 2\overline{S}_3$	$x^6+x^4+x^3+x+1$
3	$-\overline{S}_0 - 2\overline{S}_4$	$x^6+x^5+x^4+x^2+1$
4	$\overline{S}_0 - 2\overline{S}_3 + 2\overline{S}_4$	$x^6+x^4+x^3+x+1$
5	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_3$	x^6+x+1
6	$-\overline{S}_0 - 2\overline{S}_1$	$x^6+x^5+x^4+x^2+1$
7	$\overline{S}_0 + 2\overline{S}_1 + 2\overline{S}_3$	x^6+x^3+1
8	$\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_3$	$x^6+x^4+x^3+x+1$
9	$\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2 + 2\overline{S}_3 - 2\overline{S}_4$	x^3+x+1
10	$\overline{S}_0 - 2\overline{S}_2 - 2\overline{S}_3$	x^6+x+1
11	$-\overline{S}_0 + 2\overline{S}_1$	$x^6+x^5+x^2+x+1$
12	$-\overline{S}_0 - 2\overline{S}_2$	$x^6+x^5+x^4+x^2+1$
13	$-\overline{S}_0 - 2\overline{S}_4$	$x^6+x^5+x^4+x+1$
14	$\overline{S}_0 + 2\overline{S}_2 + 2\overline{S}_3$	x^6+x^3+1
15	$\overline{S}_0 + 2\overline{S}_3 - 2\overline{S}_4$	$x^6+x^4+x^2+x+1$
16	$\overline{S}_0 + 2\overline{S}_2 - 2\overline{S}_3$	$x^6+x^4+x^3+x+1$
17	$\overline{S}_0 - 2\overline{S}_2 - 2\overline{S}_3$	x^6+x+1
18	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2 + 2\overline{S}_3 - 2\overline{S}_4$	x^3+x+1
19	$-\overline{S}_0 - 2\overline{S}_1$	$x^6+x^5+x^4+x+1$
20	$\overline{S}_0 - 2\overline{S}_3 - 2\overline{S}_4$	x^6+x+1
21	$-\overline{S}_0 + 2\overline{S}_1 + 2\overline{S}_2 + 2\overline{S}_4$	x^2+x+1
22	$-\overline{S}_0 + 2\overline{S}_2$	$x^6+x^5+x^2+x+1$
23	$-\overline{S}_0 + 2\overline{S}_1$	x^6+x^5+1
24	$-\overline{S}_0 - 2\overline{S}_4$	$x^6+x^5+x^4+x^2+1$
25	$-\overline{S}_0 + 2\overline{S}_1$	$x^6+x^5+x^2+x+1$
26	$-\overline{S}_0 - 2\overline{S}_1$	$x^6+x^5+x^4+x+1$
27	$\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2 - 2\overline{S}_3 - 2\overline{S}_4$	x^3+x^2+1
28	$\overline{S}_0 + 2\overline{S}_3 + 2\overline{S}_4$	x^6+x^3+1
29	$-\overline{S}_0 + 2\overline{S}_4$	x^6+x^5+1
30	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_3$	$x^6+x^4+x^2+x+1$
31	$-\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2 - 2\overline{S}_4$	$x^6+x^5+x^3+x^2+1$

Table 6.7 – $\Lambda(a, \beta^j)$ for $\tau = 9$ — Part II

j	$\Lambda(a, \beta^j)$	m_j
32	$\overline{S}_0 - 2\overline{S}_3 + 2\overline{S}_4$	$x^6 + x^4 + x^3 + x + 1$
33	$-\overline{S}_0 - 2\overline{S}_2$	$x^6 + x^5 + x^4 + x^2 + 1$
34	$\overline{S}_0 - 2\overline{S}_3 - 2\overline{S}_4$	$x^6 + x + 1$
35	$\overline{S}_0 + 2\overline{S}_3 + 2\overline{S}_4$	$x^6 + x^3 + 1$
36	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 + 2\overline{S}_3 + 2\overline{S}_4$	$x^3 + x + 1$
37	$-\overline{S}_0 + 2\overline{S}_4$	$x^6 + x^5 + x^2 + x + 1$
38	$-\overline{S}_0 - 2\overline{S}_2$	$x^6 + x^5 + x^4 + x + 1$
39	$\overline{S}_0 - 2\overline{S}_2 + 2\overline{S}_3$	$x^6 + x^4 + x^2 + x + 1$
40	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_3$	$x^6 + x + 1$
41	$-\overline{S}_0 - 2\overline{S}_4$	$x^6 + x^5 + x^4 + x + 1$
42	$-\overline{S}_0 + 2\overline{S}_1 + 2\overline{S}_2 + 2\overline{S}_4$	$x^2 + x + 1$
43	$-\overline{S}_0 + 2\overline{S}_4$	$x^6 + x^5 + 1$
44	$-\overline{S}_0 + 2\overline{S}_4$	$x^6 + x^5 + x^2 + x + 1$
45	$\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 - 2\overline{S}_3 + 2\overline{S}_4$	$x^3 + x^2 + 1$
46	$-\overline{S}_0 + 2\overline{S}_2$	$x^6 + x^5 + 1$
47	$-\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2 - 2\overline{S}_4$	$x^6 + x^5 + x^3 + x^2 + 1$
48	$-\overline{S}_0 - 2\overline{S}_1$	$x^6 + x^5 + x^4 + x^2 + 1$
49	$\overline{S}_0 + 2\overline{S}_2 + 2\overline{S}_3$	$x^6 + x^3 + 1$
50	$-\overline{S}_0 + 2\overline{S}_2$	$x^6 + x^5 + x^2 + x + 1$
51	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_3$	$x^6 + x^4 + x^2 + x + 1$
52	$-\overline{S}_0 - 2\overline{S}_2$	$x^6 + x^5 + x^4 + x + 1$
53	$-\overline{S}_0 + 2\overline{S}_2$	$x^6 + x^5 + 1$
54	$\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2 - 2\overline{S}_3 - 2\overline{S}_4$	$x^3 + x^2 + 1$
55	$-\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 + 2\overline{S}_4$	$x^6 + x^5 + x^3 + x^2 + 1$
56	$\overline{S}_0 + 2\overline{S}_1 + 2\overline{S}_3$	$x^6 + x^3 + 1$
57	$\overline{S}_0 + 2\overline{S}_3 - 2\overline{S}_4$	$x^6 + x^4 + x^2 + x + 1$
58	$-\overline{S}_0 + 2\overline{S}_1$	$x^6 + x^5 + 1$
59	$-\overline{S}_0 - 2\overline{S}_1 + 2\overline{S}_2 - 2\overline{S}_4$	$x^6 + x^5 + x^3 + x^2 + 1$
60	$\overline{S}_0 - 2\overline{S}_2 + 2\overline{S}_3$	$x^6 + x^4 + x^2 + x + 1$
61	$-\overline{S}_0 + 2\overline{S}_1 - 2\overline{S}_2 - 2\overline{S}_4$	$x^6 + x^5 + x^3 + x^2 + 1$
62	$-\overline{S}_0 - 2\overline{S}_1 - 2\overline{S}_2 + 2\overline{S}_4$	$x^6 + x^5 + x^3 + x^2 + 1$

Table 6.8 – $\Lambda(a,b)$ for $\tau = 9$ — Subfield case

m_b	$9\Lambda(a,b)$	$o(b)$
$x+1$	$4T_1(g_a \circ D_9) - 12T_1(g_a \circ D_3) + 18T_1(g_a) + 5$	1
x^2+x+1	$-2T_1(g_a \circ D_9) - 6T_1(g_a \circ D_3) + 18T_1(g_a) + 5$	3
x^3+x+1	$8T_1(g_a \circ D_3) - 6T_1(g_a) + 1$	7
x^3+x^2+1	$4T_1(g_a \circ D_9) - 4T_1(g_a \circ D_3) - 6T_1(g_a) - 3$	7
x^6+x^3+1	$4T_1(g_a \circ D_3) + 6T_1(g_a) + 5$	9
$x^6+x^4+x^2+x+1$	$8T_1(g_a \circ D_3) - 6T_1(g_a) + 1$	21
$x^6+x^5+x^4+x^2+1$	$-2T_1(g_a \circ D_9) + 2T_1(g_a \circ D_3) - 6T_1(g_a) - 3$	21
x^6+x+1	$4T_1(g_a \circ D_9) - 4T_1(g_a \circ D_3) - 6T_1(g_a) - 3$	63
$x^6+x^4+x^3+x+1$	$4T_1(g_a \circ D_9) - 8T_1(g_a \circ D_3) + 6T_1(g_a) + 1$	63
x^6+x^5+1	$-2T_1(g_a \circ D_9) - 2T_1(g_a \circ D_3) + 6T_1(g_a) + 1$	63
$x^6+x^5+x^2+x+1$	$-2T_1(g_a \circ D_9) - 2T_1(g_a \circ D_3) + 6T_1(g_a) + 1$	63
$x^6+x^5+x^3+x^2+1$	$-2T_1(g_a \circ D_9) + 2T_1(g_a \circ D_3) - 6T_1(g_a) - 3$	63
$x^6+x^5+x^4+x+1$	$-2T_1(g_a \circ D_9) + 2T_1(g_a \circ D_3) - 6T_1(g_a) - 3$	63

(a) If b is a primitive 7-th root of unity with minimal polynomial x^3+x+1 or a primitive element with minimal polynomial x^6+x+1, then

$$9\Lambda(a,b) = 8T_1(g_a \circ D_3) - 6T_1(g_a) + 1 \ .$$

(b) If b is a primitive 7-th root of unity with minimal polynomial x^3+x^2+1 or a 21-st root of unity with minimal polynomial $x^6+x^4+x^2+x+1$, then

$$9\Lambda(a,b) = 4T_1(g_a \circ D_9) - 4T_1(g_a \circ D_3) - 6T_1(g_a) - 3 \ .$$

(c) If b is a primitive 9-th root of unity with minimal polynomial x^6+x^3+1, then

$$9\Lambda(a,b) = 4T_1(g_a \circ D_3) + 6T_1(g_a) + 5 \ .$$

(d) If b is a primitive 21-st root of unity with minimal polynomial $x^6+x^5+x^4+x^2+1$, or a primitive element with minimal polynomial $x^6+x^5+x^3+x^2+1$ or $x^6+x^5+x^4+x+1$, then

$$9\Lambda(a,b) = -2T_1(g_a \circ D_9) + 2T_1(g_a \circ D_3) - 6T_1(g_a) - 3 \ .$$

(e) If b is a primitive element with minimal polynomial $x^6+x^4+x^3+x+1$, then

$$9\Lambda(a,b) = 4T_1(g_a \circ D_9) - 8T_1(g_a \circ D_3) + 6T_1(g_a) + 1 \ .$$

(f) If b is a primitive element with minimal polynomial x^6+x^5+1 or $x^6+x^5+x^2+x+1$, then

$$9\Lambda(a,b) = -2T_1(g_a \circ D_9) - 2T_1(g_a \circ D_3) + 6T_1(g_a) + 1 \ .$$

The case $\tau = 11$

We now give a few results for $\tau = 11$, the next suitable value for τ. In this case, we have $t = 10$ and $m \equiv 5 \pmod{10}$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is $f_{a,b^{32}}$. Listing all possible characterizations would not be of high interest, hence we chose to only present results valid when the coefficients a_r are not restricted to a strict subfield of $\mathbb{F}_{2^m}$.

The characterizations valid for $a_r \in \mathbb{F}_{2^m}$, that is without further restrictions on the field the coefficients a_r lie in, are summarized in the following theorem.

Theorem 6.6.7. *Let $\tau = 11$ and $m \equiv 5 \pmod{10}$.*

1. *If $b = 1$, then*
$$11\Lambda(a,b) = 4T_1(g_a \circ D_{11}) - 22T_1(g_a) - 9 \ .$$
2. *If b is a primitive 3-rd root of unity, a primitive 341-st root of unity with minimal polynomial $x^{10}+x^9+x^8+x^3+x^2+x+1$, or a primitive element with minimal polynomial $x^{10}+x^9+x^8+x^4+x^3+x^2+1$ or $x^{10}+x^9+x^8+x^6+x^5+x+1$, then*
$$11\Lambda(a,b) = -2T_1(g_a \circ D_{11}) - 1 \ .$$

The case $\tau = 13$

We now give a few results for $\tau = 13$, the next suitable value for τ. In this case, we have $t = 12$ and $m \equiv 6 \pmod{12}$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is $f_{a,b^{64}}$. As for $\tau = 11$ we only present results valid when the coefficients a_r are not restricted to a strict subfield of $\mathbb{F}_{2^m}$.

The characterizations valid for $a_r \in \mathbb{F}_{2^m}$, that is without further restrictions on the field the coefficients a_r lie in, are summarized in the following theorem.

Theorem 6.6.8. *Let $\tau = 13$ and $m \equiv 6 \pmod{12}$.*

1. *If $b = 1$, then*
$$13\Lambda(a,b) = 4T_1(g_a \circ D_{13}) - 26T_1(g_a) - 11 \ .$$
2. *If b is a primitive 15-th root of unity with minimal polynomial x^4+x+1, a primitive 819-th root of unity with minimal polynomial $x^{12}+x^9+x^8+x^5+x^4+x+1$, a primitive 1365-th root of unity with minimal polynomial $x^{12}+x^9+x^5+x^2+1$, or a primitive element with minimal polynomial $x^{12}+x^9+x^5+x^4+x^2+x+1$, $x^{12}+x^9+x^8+x^5+1$ or $x^{12}+x^9+x^8+x^6+x^3+x^2+1$, then*
$$13\Lambda(a,b) = 2T_1(g_a \circ D_{13}) + 1 \ .$$

The case $\tau = 17$

In this subsubsection we treat the case $\tau = 17$, the next suitable value for τ. In this case, we have $t = 8$ and $m \equiv 4 \pmod{8}$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is $f_{a,b^{16}}$. Contrary to the cases $\tau = 11$ and $\tau = 13$, 2 is not a primitive root modulo 17, so that t is quite small. Therefore, we provide a complete analysis of this case.

The following theorem summarizes the characterizations valid for $a_r \in \mathbb{F}_{2^m}$, $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$ and $a_r \in \mathbb{F}_{2^{\frac{m}{4}}}$. In particular, there is none valid when $a_r \in \mathbb{F}_{2^m}$, nor for $b = 1$.

Theorem 6.6.9. *Let $\tau = 17$ and $m \equiv 4 \pmod{8}$. Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$.*

1. *If b is a primitive element with minimal polynomial $x^8+x^6+x^5+x+1$ or $x^8+x^6+x^5+x^2+1$, then*
$$17\Lambda(a,b) = 2T_1(g_a \circ D_{17}) + 1 \ .$$
2. *Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{4}}}$.*
   (a) *If b is a primitive 15-th root of unity with minimal polynomial x^4+x+1, a primitive 17-th root of unity with minimal polynomial $x^8+x^5+x^4+x^3+1$, or a primitive element with minimal polynomial $x^8+x^5+x^3+x^2+1$, then*
$$17\Lambda(a,b) = 2T_1(g_a \circ D_{17}) + 1 \ .$$
   (b) *If b is a 51-st root of unity with minimal polynomial $x^8+x^4+x^3+x+1$, then*
$$17\Lambda(a,b) = 3T_1(g_a \circ D_{17}) - 17T_1(g_a) - 7 \ .$$

The case $\tau = 33$

To conclude this subsection we treat the case of the composite integer $\tau = 33$, the first suitable value for a composite value of τ. In this case, we have $t = 10$ and $m \equiv 5 \pmod{10}$. Furthermore, if $f_{a,b}$ is hyper-bent, then its dual is $f_{a,b^{32}}$.

The following theorem summarizes the characterizations valid for $a_r \in \mathbb{F}_{2^m}$, and $a_r \in \mathbb{F}_{2^{\frac{m}{5}}}$. In particular, there is none valid when $a_r \in \mathbb{F}_{2^m}$ without further restrictions, nor for $b = 1$.

Theorem 6.6.10. *Let $\tau = 33$ and $m \equiv 5 \pmod{10}$. Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{5}}}$ and $\frac{m}{5} \not\equiv 0 \pmod 5$.*

1. *If b is a primitive 31-st root of unity with minimal polynomial $x^5 + x^2 + 1$, or a primitive 341-st root of unity with minimal polynomial $x^{10} + x^8 + x^4 + x^3 + x^2 + x + 1$, then*
$$165\Lambda(a,b) = 8T_1(g_a \circ D_{33}) + 24T_1(g_a \circ D_{11}) - 88T_1(g_a \circ D_3) + 66T_1(g_a) + 5 \ .$$
2. *If b is a primitive 31-st root of unity with minimal polynomial $x^5 + x^3 + 1$, then*
$$165\Lambda(a,b) = -8T_1(g_a \circ D_{33}) + 48T_1(g_a \circ D_{11}) + 88T_1(g_a \circ D_3) - 198T_1(g_a) - 35 \ .$$
3. *If b is a primitive 31-st root of unity with minimal polynomial $x^5+x^3+x^2+x+1$, a primitive 93-rd root of unity with minimal polynomial $x^{10} + x^8 + x^3 + x + 1$, a primitive 341-st root of unity with minimal polynomial $x^{10} + x^8 + x^7 + x^5 + x^3 + x + 1$, or a primitive element with minimal polynomial $x^{10} + x^7 + 1$, $x^{10} + x^7 + x^6 + x^4 + x^2 + x + 1$ or $x^{10} + x^8 + x^7 + x^5 + 1$, then*
$$165\Lambda(a,b) = 24T_1(g_a \circ D_{11}) + 66T_1(g_a) + 45 \ .$$
4. *If b is a primitive 93-rd root of unity with minimal polynomial $x^{10} + x^5 + x^4 + x^2 + 1$, or a primitive element with minimal polynomial $x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$ or $x^{10} + x^8 + x^5 + x^4 + x^3 + x^2 + 1$, then*
$$165\Lambda(a,b) = -4T_1(g_a \circ D_{33}) + 36T_1(g_a \circ D_{11}) + 44T_1(g_a \circ D_3) - 66T_1(g_a) + 5 \ .$$
5. *If b is a primitive 93-rd root of unity with minimal polynomial $x^{10} + x^8 + x^6 + x^5 + 1$, then*
$$165\Lambda(a,b) = 4T_1(g_a \circ D_{33}) + 36T_1(g_a \circ D_{11}) - 44T_1(g_a \circ D_3) - 66T_1(g_a) - 35 \ .$$
6. *If b is a primitive 341-st root of unity with minimal polynomial $x^{10} + x^3 + x^2 + x + 1$ or $x^{10} + x^7 + x^4 + x^3 + 1$, then*
$$165\Lambda(a,b) = -8T_1(g_a \circ D_{33}) + 36T_1(g_a \circ D_{11}) + 88T_1(g_a \circ D_3) - 66T_1(g_a) + 25 \ .$$
7. *If b is a primitive 341-st root of unity with minimal polynomial $x^{10} + x^6 + x^2 + x + 1$, or a primitive element with minimal polynomial $x^{10} + x^7 + x^3 + x + 1$, then*
$$165\Lambda(a,b) = 36T_1(g_a \circ D_{11}) - 66T_1(g_a) - 15 \ .$$
8. *If b is a primitive element with minimal polynomial $x^{10} + x^7 + x^6 + x^5 + x^4 + x + 1$ or $x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, then*
$$165\Lambda(a,b) = 4T_1(g_a \circ D_{33}) + 24T_1(g_a \circ D_{11}) - 44T_1(g_a \circ D_3) + 66T_1(g_a) + 25 \ .$$

Chapter 7

(Hyper)-bent functions and (hyper-)elliptic curves

Contents

7.1 Elliptic curves and hyperelliptic curves

7.1.1 Elliptic curves over finite fields

In this subsection, we present some classical results about elliptic curves over finite fields, as well as their connections with binary Kloosterman sums.

Let m be a positive integer, $\mathbb{F}_q$ the finite field of characteristic p with $q = p^m$ and $[q]$ its algebraic closure. Let E be an elliptic curve defined over $\mathbb{F}_q$. It can be given by a Weierstrass

equation [238, Chapter III] describing its affine part as follows:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ .$$

Over an algebraically closed field, elliptic curves are classified up to isomorphism by the so-called j-invariant [238, Proposition III.1.4].

There exists an addition on the set of rational points of the curve (i.e. points with coordinates in $\mathbb{F}_q$), giving it a group structure. We denote by O_E the unique point at infinity of E, which is also the neutral point for the addition law, by $[n]$ the multiplication by an integer n on E and by $\mathrm{End}(E) = \mathrm{End}_{[q]}(E)$ the ring of endomorphisms of E over the algebraic closure $[q]$.

The group of rational points of E over an extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ is denoted by $E(\mathbb{F}_{q^k})$; the number of points of this group by $\#E(\mathbb{F}_{q^k})$. When the context is clear, we denote $\#E(\mathbb{F}_q)$ simply by $\#E$. It is a classical result that $\#E = q + 1 - t$ where t is the trace of the Frobenius automorphism of E over $\mathbb{F}_q$ [238, Remark V.2.6] and the following theorem has been shown by Hasse.

Theorem 7.1.1 ([238, Theorem V.2.3.1])**.** *Let t be the trace of the Frobenius automorphism of an elliptic curve over $\mathbb{F}_q$, then*

$$|t| \leq 2\sqrt{q} \ .$$

For an integer n, we denote by $E[n]$ the n-torsion subgroup of the points of E over $[q]$, i.e.

$$E[n] = \{P \in E([q]) \mid [n]P = O_E\} \ .$$

The subgroup of rational points of n-torsion is denoted by $E[n](\mathbb{F}_q) = E[n] \cap E(\mathbb{F}_q)$. The following classical result gives the structure of the groups of torsion points.

Proposition 7.1.2 ([238, Corollary III.6.4])**.** *Let n be a positive integer.*

- *If $p \nmid n$, then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*
- *One of the following is true: $E[p^e] \simeq \{0\}$ for all $e \geq 1$ or $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$ for all $e \geq 1$.*

It can also be shown that a point of E is of n-torsion if and only if its coordinates are roots of a bivariate polynomial called the n-division polynomial of E [6, Section III.4]. In fact one can even choose a univariate polynomial in the x-coordinate that we denote by f_n.

Here we will be interested in *ordinary* elliptic curves which can be defined as follows.

Definition 7.1.3 ([238, Theorem V.3.1])**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$ and t the trace of the Frobenius automorphism of E. E is said to be ordinary if it verifies one of the following equivalent properties:*

- *$p \nmid t$;*
- *$E[p] \simeq \mathbb{Z}/p\mathbb{Z}$;*
- *$\mathrm{End}(E)$ is an order [1] in an imaginary quadratic extension of $\mathbb{Q}$.*

[1] An order $\mathcal{O}$ in a number field K is a subring of the ring of integers $\mathcal{O}_K$ which generates the number field over $\mathbb{Q}$. In an imaginary quadratic field, it can be uniquely written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ where $f \in \mathbb{N}^*$ is a positive integer and is called the *conductor* of $\mathcal{O}$. Reciprocally, each possible conductor gives an order in an imaginary quadratic field.

If E is not ordinary, it is said to be *supersingular*.

Finally, using classical results of Deuring [81] and Waterhouse [261], the number of ordinary elliptic curves (up to isomorphism) with a given trace t of the Frobenius automorphism (or equivalently a number of points $q+1-t$), verifying $|t| \leq 2\sqrt{q}$ and $p \nmid t$, can be computed as follows. This property indeed implies that $\mathrm{End}(E)$ must be an order $\mathcal{O}$ in $K = \mathbb{Q}[\alpha]$ and contains the order $\mathbb{Z}[\alpha]$ of discriminant Δ where $\alpha = \frac{t+\sqrt{\Delta}}{2}$ and $\Delta = t^2 - 4q$. We denote by $H(\Delta)$ the *Kronecker class number* [232, 76]

$$H(\Delta) = \sum_{\mathbb{Z}[\alpha] \subset \mathcal{O} \subset K} h(\mathcal{O}) \ ,$$

where the sum is taken over all the orders $\mathcal{O}$ in K containing $\mathbb{Z}[\alpha]$ and $h(\mathcal{O})$ is the classical class number.

Proposition 7.1.4 ([232, 146, 76])**.** *Let t be an integer such that $|t| \leq 2\sqrt{q}$ and $p \nmid t$. The number $N(t)$ of elliptic curves over $\mathbb{F}_q$ with $q+1-t$ rational points is given by*

$$N(t) = H(\Delta) \ ,$$

where $\Delta = t^2 - 4q$.

It should be noted that $H(\Delta)$ can be computed from the value of the classical class number of (the ring of integers of) K using the following proposition.

Proposition 7.1.5 ([158, 76, 146, 70])**.** *Let $\mathcal{O}$ be the order of conductor f in K, an imaginary quadratic extension of $\mathbb{Q}$, , $\mathcal{O}_K$ the ring of integers of K and Δ_K the discriminant of (the ring of integers of) K. Then*

$$h(\mathcal{O}) = \frac{f h(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p \mid f} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right) \ ,$$

where $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

Denoting the conductor of $\mathbb{Z}[\alpha]$ by f, $H(\Delta)$ can then be written as

$$H(\Delta) = h(\mathcal{O}_K) \sum_{d \mid f} \frac{d}{[\mathcal{O}_K^* : \mathcal{O}]} \prod_{p \mid d} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right) \ .$$

We now give specific results to even characteristic. First, E is supersingular if and only if its j-invariant is 0. Second, if E is ordinary, then its Weierstrass equation can be chosen to be of the form

$$E : y^2 + xy = x^3 + bx^2 + a \ ,$$

where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, its j-invariant is then $1/a$; moreover its first division polynomials are given by [153, 6]

$$f_1(x) = 1, \quad f_2(x) = x, \quad f_3(x) = x^4 + x^3 + a, \quad f_4(x) = x^6 + ax^2 \ .$$

The quadratic twist of E is an elliptic curve with the same j-invariant as E, so isomorphic over the algebraic closure $[q]$, but not over $\mathbb{F}_q$ (in fact it becomes so over $\mathbb{F}_{q^2}$). It is unique up to isomorphism and we denote it by $\widetilde{E}$. It is given by the Weierstrass equation

$$\widetilde{E} : y^2 + xy = x^3 + \widetilde{b}x^2 + a \ ,$$

where $\widetilde{b}$ is any element of $\mathbb{F}_q$ such that $\mathrm{Tr}_1^m\left(\widetilde{b}\right) = 1 - \mathrm{Tr}_1^m(b)$ [97]. The trace of its Frobenius automorphism is given by the opposite of the trace of the Frobenius automorphism of E, so that their number of rational points are closely related [97, 6]:

$$\#E + \#\widetilde{E} = 2q + 2 \ .$$

7.1.2 Hyperelliptic curves et point counting

In this section we give basic definitions and results for hyperelliptic curves with a special emphasis on point counting on such curves over finite fields of even characteristic. For a general overview of the theory of such curves, with a cryptographic point of view, the reader is referred to the textbooks of Cohen et al. [71] or that of Galbraith [109].

For our purposes, it is enough to consider *imaginary* hyperelliptic curves. Imaginary hyperelliptic curves are smooth projective curves whose affine part can be described by an equation of the form

$$H : y^2 + h(x)y = f(x) \ ,$$

where $h(x)$ is a polynomial of degree $\leq g$, the genus of the curve, and $f(x)$ is a monic polynomial of degree $2g + 1$. They have exactly one point at infinity. Curves for which $h(x) = x^k$, where $0 \leq k \leq g$, are called Artin–Schreier curves. The case $g = 1$ corresponds to elliptic curves.

The number of points on a hyperelliptic curve H over the finite field $\mathbb{F}_{2^m}$ is understood as its numbers of points with coordinates in the finite field $\mathbb{F}_{2^m}$, which are also called $\mathbb{F}_{2^m}$*-rational points*. It is denoted by $\#H(\mathbb{F}_{2^m})$. The reference to the finite field is usually omitted when the context makes it clear.

A very important result is that there exist algorithms to compute this number of points in polynomial time and space in m. Such a result has been given by Denef and Vercauteren who extended a previous result of Kedlaya [148] in odd characteristic.

Theorem 7.1.6 ([253, Theorem 4.4.1], [80])**.** *Let H be an imaginary hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the number of points on H in*

$$O(g^{5+\epsilon}m^{3+\epsilon})$$

bit operations and $O(g^4m^3)$ memory, where $\epsilon \in \Re_+^*$ is any strictly positive real number.

A slightly stronger result is true for Artin–Schreier curves.

Theorem 7.1.7 ([253, Theorem 4.3.1],[79])**.** *Let H be an Artin–Schreier curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the number of points on H in*

$$O(g^{5+\epsilon}m^{3+\epsilon})$$

bit operations and $O(g^3m^3)$ memory, where $\epsilon \in \Re_+^*$ is any strictly positive real number.

Better complexities were recently obtained through the use of complex methods involving deformation theory. For example, Hubrechts obtained the following result.

Theorem 7.1.8 ([135, Theorem 2])**.** *Let H be an hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the number of points on H in*

$$O(g^{7.376}m^2 + g^{3.376}m^{2.667})$$

bit operations and $O(g^5m^2 + g^3m^{2.5})$ memory.

In fact such algorithms are even more interesting when one wants to compute the number of points on several curves within the same family.

To conclude, let us mention the existence of a quasi-quadratic algorithm described by Lercier and Lubicz [162].

Theorem 7.1.9. *Let H be a hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(2^{4g+o(1)}g^3m^{2+o(1)})$$

bit operations and $O(2^{3g+o(1)}m^2)$ memory.

Nevertheless, it should be remarked that the time and space complexities of this last algorithm are exponential in the genus of the curve and so it is of practical interest for curves of relatively genera only.

7.2 Exponential sums and algebraic varieties

7.2.1 Kloosterman sums and elliptic curves

The idea to connect Kloosterman sums and elliptic curves goes back to the works of Lachaud and Wolfmann [157], and Katz and Livné [146]. We recall a simple proof of their main result in a simpler and less general formulation here. Indeed, its generalizations which will be covered in the next subsection can be proved in a very similar manner.

Theorem 7.2.1 ([157, 146])**.** *Let $m \geq 3$ be any positive integer, $a \in \mathbb{F}_{2^m}^*$ and E_a the projective elliptic curve defined over $\mathbb{F}_{2^m}$ whose affine part is given by the equation*

$$E_a : \ y^2 + xy = x^3 + a \ .$$

Then

$$\#E_a = 2^m + K_m(a) \ .$$

Proof. Indeed

$$K_m(a) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) \ ,$$

and

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) &= \sum_{x \in \mathbb{F}_{2^m}^*} \left(1 - 2\,\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) \\ &= 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1} + ax\right) = 1\right\} \\ &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1} + ax\right) = 0\right\} \ .\end{aligned}$$

Using the additive version of Hilbert's Theorem 90, we get

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) = -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = x^{-1} + ax\right\} \ ,$$

and applying the substitution $t = t/x$ we get

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ (t/x)^2 + (t/x) = x^{-1} + ax\right\} \\ &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + xt = x + ax^3\right\} \ .\end{aligned}$$

We recognize the number of points of E_a minus the only point with x-coordinate $x = 0$ and the only point at infinity.

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1} + ax\right)\right) &= -2^m + 1 + \#E_a - 2 \\ &= -2^m - 1 + \#E_a \ .\end{aligned}$$ □

Hence, the necessary and sufficient condition for hyper-bentness of the monomial functions with the Dillon exponent can be reformulated as follows.

Proposition 7.2.2 (Reformulation of the Dillon criterion)**.** *The notation is as in Theorem 7.2.1. Moreover, let r be an integer such that $\gcd(r, 2^m + 1) = 1$ and f_a be the Boolean function with n inputs defined as $f_a(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$. Then f_a is hyper-bent if and only if*

$$\#E_a = 2^m \ .$$

7.2.2 Exponential sums and hyperelliptic curves

In the two following propositions we link exponential sums with cardinalities of hyperelliptic curve, which will be of interest later on.

Proposition 7.2.3. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $f(0) = 0$, $g = \mathrm{Tr}_1^m(f)$, and G_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$G_f : y^2 + y = f(x) \ .$$

Then

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) = -2^m - 1 + \#G_f \ .$$

Proof. The first step of the proof is to express $\chi(g(x))$ as $1 - 2g(x)$ where $g(x)$ is now understood to be integer-valued:

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) = \sum_{x \in \mathbb{F}_{2^m}^*} (1 - 2g(x)) \ .$$

The sum can then be split according to the value of $g(x)$ yielding the equality

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) = 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid g(x) = 1\right\} \ .$$

We supposed that $g(0) = 0$, so we can include zero in the summation set in the right hand side of the previous equality and deduce

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) &= 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m} \mid g(x) = 1\right\} \\ &= 2^m - 1 - 2\left(2^m - \#\left\{x \in \mathbb{F}_{2^m} \mid g(x) = 0\right\}\right) \\ &= -2^m - 1 + 2\#\left\{x \in \mathbb{F}_{2^m} \mid g(x) = 0\right\} \ .\end{aligned}$$

The additive version of Hilbert's Theorem 90 characterizes elements of trace zero as those which can be written as $t + t^2$ so that we get the equivalent formulation

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g(x)\right) = -2^m - 1 + 2\#\left\{x \in \mathbb{F}_{2^m} \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = f(x)\right\} \ .$$

The last term of the right hand side of the above equality is nothing but the number of $\mathbb{F}_{2^m}$-rational (affine) points of G_f, whence

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g(x)\right) = -2^m - 1 + \#G_f \ ,$$

which concludes the proof of the proposition. □

Proposition 7.2.4. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function, $g = \mathrm{Tr}_1^m(f)$, and H_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$H_f : y^2 + xy = x + x^2 f(x) \ ,$$

Then

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m(1/x) + g(x)\right) = -2^m + \#H_f \ .$$

Proof. The proof is quite similar as that of Proposition 11.0.1. It begins with the same sequence of equalities:

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m(1/x) + g(x)\right) &= \sum_{x \in \mathbb{F}_{2^m}^*} \left(1 - 2(\mathrm{Tr}_1^m(1/x) + g(x))\right) \\
&= 2^m - 1 - 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m(1/x) + g(x) = 1\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m(1/x) + g(x) = 0\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + t = 1/x + f(x)\right\} \ .
\end{aligned}$$

The additional step is then to substitute t by t/x before clearing denominators, which is legal since x is non-zero, before finishing the proof using the same arguments.

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m(1/x) + g(x)\right) &= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ (t/x)^2 + (t/x) = 1/x + f(x)\right\} \\
&= -2^m + 1 + 2\#\left\{x \in \mathbb{F}_{2^m}^* \mid \exists t \in \mathbb{F}_{2^m},\ t^2 + xt = x + x^2 f(x)\right\} \\
&= -2^m + 1 + \#H_f - \#\left\{P \in H_f \mid x = 0\right\} \\
&= -2^m + \#H_f \ .
\end{aligned}$$

□

Proposition 11.0.1 and Proposition 11.0.2 give the following reformulation of Lemma 2.4.8 in terms of curves.

Corollary 7.2.5. *The notation is as in Proposition 7.3.8. Then*

$$T_i(g) = \frac{1}{2}\left((\#G_f - 2^m) + (-1)^i(\#H_f - 2^m + 1)\right) \ .$$

When applied to Corollary 2.4.9, we get the following interesting result about curves.

Corollary 7.2.6. *The notation is as in Proposition 7.3.8. Let moreover $1 \leq r \leq 2^n - 1$ be an integer such that $\gcd(r, 2^m - 1) = 1$. Then*

$$\#H_f^r + \#G_f^r = \#H_f + \#G_f \ .$$

7.3 Efficient characterizations of hyper-bentness: reformulation in terms of cardinalities of curves

7.3.1 Efficient characterizations of hyper-bentness: the Charpin and Gong criterion

Thanks to Proposition 11.0.1 and Proposition 11.0.2 we can now easily deduce the reformulation of the Charpin–Gong criterion given by Lisoněk.

Theorem 7.3.1 (Reformulation of the Charpin–Gong criterion [170])**.** *Let E' be a set of representatives of the cyclotomic cosets modulo 2^m+1 for which each coset has the maximal size n. Let f_{a_r} be the function of $\mathcal{F}_n$ defined on $\mathbb{F}_{2^n}$ by $f_a(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$ where $a_r\in\mathbb{F}_{2^n}$ and $R\subseteq E'$. Moreover, let H_a and G_a be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$G_a : y^2+y=\sum_{r\in R} a_r D_r(x) \ ,$$
$$H_a : y^2+xy=x+x^2\sum_{r\in R} a_r D_r(x) \ .$$

Then f_a is hyper-bent if and only if

$$\#H_a-\#G_a=-1 \ .$$

Proof. According to Proposition 11.0.2, the left hand side of the Charpin–Gong criterion satisfies

$$\sum_{x\in\mathbb{F}_{2^m}^*}\chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_a(x)\right)=-2^m+\#H_a \ ;$$

and, according to Proposition 11.0.1, the right hand side of the Charpin–Gong criterion satisfies

$$\sum_{x\in\mathbb{F}_{2^m}^*}\chi\left(g_a(x)\right)=-2^m-1+\#G_a \ . \qquad \square$$

As a consequence of this corollary, Lisoněk obtained a polynomial time and space test for hyper-bentness of Boolean functions in the Charpin–Gong family. Let r_{max} the maximal index in R, which can be supposed to be odd, and will be for two reasons:

1. it ensures that the curves H_a and G_a are imaginary hyperelliptic curves;
2. as will be discussed below, r_{max} should be as small as possible for efficiency reasons, so the natural choice for the indices in a cyclotomic coset will be the coset leaders which are odd integers.

In fact, the curves G_a and H_a are even Artin–Schreier curves. Theorems 7.1.7 and 7.1.8 state that there exist efficient algorithms to compute the cardinality of such curves as long as r_{max} is supposed to be relatively small. The polynomial defining H_a (respectively G_a) is indeed of degree $r_{max}+2$ (respectively r_{max}), so the curve is of genus $(r_{max}+1)/2$ (respectively $(r_{max}-1)/2$). The complexity for testing the hyper-bentness of a Boolean function in this family is then dominated by the computation of the cardinality of a curve of genus $(r_{max}+1)/2$. Then, applying Theorem 7.1.8 gives the following time and space complexities in m and r_{max}.

Theorem 7.3.2. *Let f_a be a function in the family $\mathcal{F}_n$ defined as above. Let moreover r_{max} be the maximal index in R. Then the hyper-bentness of f_a can be checked in*

$$O(r_{max}^{7.376} m^2 + r_{max}^{3.376} m^{2.667})$$

bit operations and $O(r_{max}^5 m^2 + r_{max}^3 m^{2.5})$ memory.

Therefore, if R is supposed to be fixed, then so are r_{max} and the genera of the curves G_a and H_a, and the complexities of Theorem 7.3.21 are indeed polynomial in m as stated by Lisoněk [170, Theorem 5]. Asymptotically, this is much better than a straightforward application of Theorem 6.1.1 where the exponential sums on $\mathbb{F}_{2^m}$ are naively computed one term at a time. Indeed, for each of the 2^{m-1} terms of the partial exponential sums over $\mathcal{T}_1$, one has to compute the function $g_a(x) = \sum_{r \in R} \mathrm{Tr}_1^m (a_r D_r(x))$. The time complexity of this computation is dominated by the cost of a constant number of multiplications in $\mathbb{F}_{2^m}$. Therefore, the total time complexity is $O(2^m m^{1+\epsilon})$ and the space complexity is $O(m)$, where $\epsilon \in \Re_+^*$ is any strictly positive real number. Testing hyper-bentness through a naive computation of $\Lambda(f_a)$ yields similar complexity, although the arithmetic takes place in $\mathbb{F}_{2^n}$ rather than $\mathbb{F}_{2^m}$.

It should be remarked that if no restriction is cast upon R, then the maximal index r_{max} will obviously depend on m and will in fact grow, at least, as $2^m/m$. It is indeed sufficient to note that this is true when m is prime. Then, each non-trivial cyclotomic coset has indeed size dividing $n = 2m$. It has size 2 if and only if $3r \equiv 0 \pmod{2^m + 1}$ for $0 \leq r \leq 2^m$, i.e. $3r = 2^m + 1$ or $3r = 2(2^m + 1)$. Hence, there are exactly one such class when $3 \mid 2^m + 1$, that is when m is odd, and no such class otherwise. The size of the other cosets is then $2m$, so that the largest coset leader, which is odd, is at least $(2^m - 2)/m$.

Consequently, the time and space complexities of Theorem 7.3.21 will become exponential, whereas the time complexities of the naive approaches will become $O(2^m m^{2+\epsilon})$ (now dominated by the computation of an exponentation with an arbitrary large exponent), where $\epsilon \in \Re_+^*$ is any strictly positive real number, and their space complexities will not change.

Nonetheless, fixing a set R, i.e. only looking for Boolean functions with a given polynomial form within a large family, is customary in cryptographic applications. Moreover, experimental data provided by Lisoněk [170, Table 1] and in Subsection 7.3.4 show that such reformulations also have a practical impact, so that the above approach seem meaningful.

7.3.2 Efficient characterizations of hyper-bentness: our criterion

We now show that a similar reformulation can be applied to the different versions of our criterion for Boolean functions with multiple trace terms.

Theorem 7.3.3 (Reformulation of the hyper-bentess criterion for functions in $\mathfrak{H}_n$)**.** *Let $f_{a,b}$ be a function of $\mathfrak{H}_n$ defined by $f_{a,b}(x) := \sum_{r \in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(b x^{\frac{2^n-1}{3}})$. Moreover, let H_a and G_a be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$G_a : y^2 + y = \sum_{r \in R} a_r D_r(x) \ ,$$
$$H_a : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(x) \ ;$$

and let H_a^3 *and* G_a^3 *be the (affine) curves defined over* $\mathbb{F}_{2^m}$ *by*

$$G_a^3 : y^2 + y = \sum_{r \in R} a_r D_r(D_3(x)) \ ,$$
$$H_a^3 : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(D_3(x)) \ .$$

If b *is a primitive element of* $\mathbb{F}_4$*, then* $f_{a,b}$ *is hyper-bent if and only if*

$$\#H_a^3 - \#G_a^3 = 3 \ .$$

If $b = 1$*, then* $f_{a,1}$ *is hyper-bent if and only if*

$$\left(\#G_a^3 - \#H_a^3\right) - \frac{3}{2}\left(\#G_a - \#H_a\right) = \frac{3}{2} \ .$$

Proof. If b is a primitive element of $\mathbb{F}_4$, according to Proposition 11.0.2 the left hand side of Condition (c)-(iii) of Theorem 6.2.10 satisfies

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(D_3(x))\right) = -2^m + \#H_a^3 \ ,$$

and according to Proposition 11.0.1 the right hand side of Condition (c)-(iii) of Theorem 6.2.10 satisfies

$$2^m - 2\,\mathrm{w_H}(g_a \circ D_3) + 3 = -2^m + 3 + \#G_a^3 \ ,$$

so that the criterion is equivalent to

$$\#H_a^3 - \#G_a^3 = 3 \ .$$

We could also have used Condition (c)-(ii) of Theorem 6.2.10 and that its left hand side satisfies

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m\left(x^{-1}\right)=1} \chi\left(g_a \circ D_3(x)\right) &= \frac{1}{2}\left(\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(g_a \circ D_3(x)\right) - \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a \circ D_3(x)\right)\right) \\ &= \frac{1}{2}\left(\left(-2^m - 1 + \#G_a^3\right) - \left(-2^m + \#H_a^3\right)\right) \\ &= \frac{1}{2}\left(\#G_a^3 - \#H_a^3 - 1\right) \ ;\end{aligned}$$

and decuce the same reformulation.

If $b = 1$, using the previous calculations, the first term in Condition (d) of Theorem 6.2.10 satisfies

$$2 \sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a \circ D_3(x)\right) = \#G_a^3 - \#H_a^3 - 1 \ ;$$

and the second term satisfies

$$3 \sum_{x \in \mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a(x)\right) = \frac{3}{2}\left(\#G_a - \#H_a - 1\right) \ ;$$

whence the reformulation. □

Here all the curves are also Artin–Schreier curves. So, for a fixed subset of indices R, we also get a test in polynomial time and space in m. However, the complexity of the point counting algorithms also depends on the genera of the curves, and so on the degrees of the polynomials defining them. Denoting by r_{max} the maximal index as above, the genus of H_a^3 (respectively G_a^3) is $(3r_{max}+1)/2$ (respectively $(3r_{max}-1)/2$), so approximately three times that of H_a (respectively G_a). Therefore, the associated test will be much slower than for Boolean functions of the family of Charpin and Gong for a given subset R: we have to compute the cardinalities of two curves of genera $(3r_{max}+1)/2$ and $(3r_{max}-1)/2$ if b is primitive, or four curves of genera $(3r_{max}+1)/2$, $(3r_{max}-1)/2$, $(r_{max}+1)/2$ and $(r_{max}-1)/2$ if $b=1$, instead of two curves of genera $(r_{max}+1)/2$ and $(r_{max}-1)/2$. Hence, we propose another reformulation of our criterion involving slightly less computations.

Theorem 7.3.4 (Second reformulation of the hyper-bentness criterion for functions in $\mathfrak{H}_n$)**.** *Let $f_{a,b}$ be a function of the family $\mathfrak{H}_n$ defined as above. If b is a primitive element of $\mathbb{F}_4$, then $f_{a,b}$ is hyper-bent if and only if*

$$\#G_a^3 - \frac{1}{2}\left(\#G_a + \#H_a\right) = -\frac{3}{2} \ .$$

If $b=1$, then $f_{a,1}$ is hyper-bent if and only if

$$2\#G_a^3 - \frac{5}{2}\#G_a + \frac{1}{2}\#H_a = \frac{3}{2} \ .$$

Proof. We use the fact that m is odd, so that the function $x \mapsto D_3(x) = x^3 + x$ is a permutation of the set $\left\{x \in \mathbb{F}_{2^m}^* \mid \mathrm{Tr}_1^m\left(x^{-1}\right) = 0\right\}$ (see the papers of Berlekamp, Rumsey and Solomon [5, Theorem 2] and Charpin, Helleseth and Zinoviev [60] for the case of D_3, or more generally the article of Dillon and Dobbertin [88]), and similar arguments as previously.

If b is a primitive element of $\mathbb{F}_4$, then the left hand side in Condition (c)-(ii) of Theorem 6.2.10 satisfies

$$\begin{aligned}
\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a \circ D_3(x)\right) &= \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a \circ D_3(x)\right) - \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=0} \chi\left(g_a \circ D_3(x)\right) \\
&= \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a \circ D_3(x)\right) - \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=0} \chi\left(g_a(x)\right) \\
&= \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a \circ D_3(x)\right) \\
&\quad - \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(g_a(x)\right) + \sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_a(x)\right)\right) \\
&= \left(-2^m - 1 + \#G_a^3\right) - \frac{1}{2}\left(\left(-2^m - 1 + \#G_a\right) + \left(-2^m + \#H_a\right)\right) \\
&= -\frac{1}{2} + \#G_a^3 - \frac{1}{2}\left(\#G_a + \#H_a\right) \ .
\end{aligned}$$

If $b=1$, then the first term in Condition (d) of Theorem 6.2.10 satisfies

$$2\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_a \circ D_3(x)\right) = -1 + 2\#G_a^3 - \left(\#G_a + \#H_a\right) \ . \qquad \square$$

Here we discarded the computation of the cardinality of the curve of genus $(3r_{max}+1)/2$ and we have to compute the cardinalities of three curves of genera $(3r_{max}-1)/2$, $(r_{max}+1)/2$ and $(r_{max}-1)/2$.

Table 7.1 – Meantimes needed to compute the number of points on G_a, H_a, G_a^3 and H_a^3

m	$\#G_a$	$\#H_a$	$\#G_a^3$	$\#H_a^3$	m	$\#G_a$	$\#H_a$	$\#G_a^3$	$\#H_a^3$
21	0.017	0.488	6.857	13.894	41	0.018	1.868	40.877	108.704
23	0.016	0.576	8.736	16.021	43	0.018	2.575	47.010	128.340
25	0.017	0.653	10.587	20.287	45	0.019	4.986	62.107	176.841
27	0.016	0.912	13.684	25.704	47	0.019	5.663	84.905	210.458
29	0.017	0.869	14.843	27.667	49	0.019	6.532	94.532	234.329
31	0.016	1.026	17.766	34.532	51	0.019	7.982	125.468	242.358
33	0.017	1.166	31.258	59.000	53	0.019	7.676	133.737	249.522
35	0.018	1.317	26.809	57.998	55	0.019	8.437	116.552	275.870
37	0.018	1.562	33.321	79.949	57	0.020	9.504	127.507	305.787
39	0.019	1.893	46.768	99.544	59	0.020	9.881	162.632	360.508

we have shown how our criterion can be reformulated in terms of cardinalities of hyperelliptic curves; we now study the practical impact of such reformulations.

To begin with, even though the overall complexity is not changed between the two reformulations we presented, the practical difference is non-negligible. To illustrate this fact, we performed several simulations with Magma v2.17-13 [8]. The computations were performed on an Intel Core2 Quad CPU Q6600 cadenced at 2.40 GHz. The set R of indices used was $R = \{1, 3\}$ and one hundred of couples of coefficients (a_1, a_3) were randomly generated in $\mathbb{F}_{2^m}^*$. The meantimes (in seconds) needed to compute the number of points on the curves G_a, H_a, G_a^3 and H_a^3 for odd integers m between 21 and 59 are presented in Table 7.3. These data show that using the second reformulation is roughly twice as fast as using the first one. It also confirms that testing a function in our family using such a reformulation is much slower than testing a function in the Charpin–Gong family.

Table 7.2 shows how the second reformulation compares with a straightforward application of more classical characterizations involving exponential sums where the given sums are computed one term at a time. The column Λ indicates the meantimes (in seconds) needed to check the hyper-bentness of a function $f_{a,b}$ in our family by computing naively the exponential sum $\Lambda(f_{a,1})$, the column $\mathcal{T}_i$ by computing naively the exponential sums on $\mathcal{T}_i$ of Theorem 6.2.10, and the column $\#H$ by using the second reformulation of the previous section, for $b = 1$ and ten random pairs (a_1, a_3) of coefficients in $\mathbb{F}_{2^m}$ for m from 1 to 29, and only one couple (a_1, a_3) for m from 31 to 59. Two remarks should be made about the data exposed in Table 7.2. First, it should be noted that Magma actually uses a *naive* point counting based on exponential sums for m up to 20 where it switches to the Denef–Vercauteren algorithm mentioned in Theorem 7.1.6. Nonetheless, the fact that a naive point counting algorithm has an exponential time complexity and the experimental data provided in Table 7.2 show that using such an algorithm for m greater than 20 would not be beneficial. Second, it is clear that the reformulations in terms of hyperelliptic curves are of practical interest, for relatively small values of m, and for values of m of cryptographic interest.

As a final piece of experimental evidence, the second reformulation made it possible to find hyper-bent functions of cryptographic size in our family, even though the tests are much slower than the corresponding ones for functions in the Charpin–Gong family. A random search on pairs (a_1, a_3) as above indeed showed that the Boolean functions associated with the following coefficients[2] are hyper-bent (the finite field $\mathbb{F}_{2^m}$ is represented as $\mathbb{F}_2[x]$ quotiented by the ideal generated by the m-th binary Conway polynomial):

[2]Recall that the coefficient a_1 and a_3 are defined over $\mathbb{F}_{2^m}$, but that the corresponding Boolean functions have $n = 2m$ inputs.

Table 7.2 – Meantimes needed to test the hyper-bentness of $f_{a,1}$

m	Λ	$\mathcal{T}_i$	$\#H$	m	Λ	$\mathcal{T}_i$	$\#H$
1	0.000	0.000	0.000	31	23213.840	29521.440	18.460
3	0.000	0.000	0.000	33	109889.470	119733.320	29.030
5	0.000	0.000	0.000	35	445344.020	490439.190	25.750
7	0.001	0.001	0.000	37	−−	−−	33.631
9	0.003	0.003	0.002	39	−−	−−	46.898
11	0.019	0.011	0.004	41	−−	−−	40.585
13	0.073	0.042	0.018	43	−−	−−	46.713
15	0.301	0.166	0.076	45	−−	−−	63.693
17	1.165	0.658	0.300	47	−−	−−	86.434
19	4.571	2.693	1.277	49	−−	−−	95.525
21	20.863	24.376	6.893	51	−−	−−	127.055
23	76.744	99.918	8.769	53	−−	−−	133.471
25	330.874	410.432	10.642	55	−−	−−	116.726
27	1371.403	1716.147	13.914	57	−−	−−	127.596
29	5472.347	6794.873	14.799	59	−−	−−	161.185

- for $b = 0$, the pair

$$\begin{aligned} a_1 &= x^{34} + x^{31} + x^{29} + x^{27} + x^{26} + x^{24} + x^{23} + x^{21} + x^{20} + x^{18} + x^{17} + x^{16} \\ &\quad + x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 \ , \\ a_3 &= x^{32} + x^{29} + x^{27} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{18} + x^{16} + x^{12} + x^8 \\ &\quad + x^4 + x \ , \end{aligned}$$

  in $\mathbb{F}_{2^{35}}$ represented as $\mathbb{F}_2[x]/\left(x^{35} + x^{11} + x^{10} + x^7 + x^5 + x^2 + 1\right)$;

- for $b = 1$, the pair

$$\begin{aligned} a_1 &= x^{27} + x^{26} + x^{25} + x^{24} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} \\ &\quad + x^{14} + x^{13} + x^{11} + x^7 + x^5 + x^4 + x^2 + 1 \ , \\ a_3 &= x^{30} + x^{29} + x^{27} + x^{26} + x^{22} + x^{20} + x^{17} + x^{16} + x^{15} + x^{12} + x^{10} + x^4 \\ &\quad + x^3 + x^2 \ , \end{aligned}$$

  in $\mathbb{F}_{2^{33}}$ represented as $\mathbb{F}_2[x]/\left(x^{33} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^3 + 1\right)$;

- for $b = \beta$ a primitive element of $\mathbb{F}_4$, the pair

$$\begin{aligned} a_1 &= x^{32} + x^{31} + x^{29} + x^{27} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{15} \\ &\quad + x^{11} + x^{10} + x^9 + x^3 + x^2 + x \ , \\ a_2 &= x^{32} + x^{29} + x^{28} + x^{27} + x^{26} + x^{24} + x^{22} + x^{18} + x^{17} + x^{13} + x^{10} + x^8 \\ &\quad + x^7 + x^6 + x^5 + x^4 \ , \end{aligned}$$

  in $\mathbb{F}_{2^{33}}$ represented as $\mathbb{F}_2[x]/\left(x^{33} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^3 + 1\right)$.

7.3.3 Efficient characterizations of hyper-bentness: the Wang et al. criterion

Finally, we extend the previous works to reformulate the characterizations given by Wang et al. in terms of the number of points on hyperelliptic curves and present some numerical results leading to an interesting problem.

Applying Corollary 7.3.9 to Theorem 6.6.5 leads to the following reformulation.

Theorem 7.3.5. *The notation is as in Theorem 6.6.5, Proposition 11.0.1 and Proposition 11.0.2*

1. *If $b = 1$, then $5\Lambda(f_{a,1}) = 2(\#G_a^5 - \#H_a^5) - 5(\#G_a - \#H_a)$.*
2. *If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, then $5\Lambda(f_{a,b}) = \#G_a^5 - \#H_a^5$.*
3. *If moreover $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$, then*
   (a) *if b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 1$, then $10\Lambda(f_{a,b}) = -3(\#G_a^5 - \#H_a^5) + 5(\#G_a - \#H_a)$;*
   (b) *if b is a primitive 5-th root of unity, then $10\Lambda(f_{a,b}) = -(\#G_a^5 - \#H_a^5) - 5(\#G_a - \#H_a)$;*
   (c) *if b is a primitive 3-rd root of unity, then $5\Lambda(f_{a,b}) = \#G_a^5 - \#H_a^5$.*

Applying Corollary 7.3.10 then yields a more practical reformulation for explicit generation of hyper-bent functions.

Theorem 7.3.6. *The notation is as in Theorem 7.3.5.*

1. *If $b = 1$, then $5\Lambda(f_{a,1}) = 4\#G_a^5 - 7\#G_a + 3\#H_a$.*
2. *If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, then $5\Lambda(f_{a,b}) = 2\#G_a^5 - \#G_a - \#H_a$.*
3. *If moreover $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$, then*
   (a) *if b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 1$, then $5\Lambda(f_{a,b}) = -3\#G_a^5 + 4\#G_a - \#H_a$;*
   (b) *if b is a primitive 5-th root of unity, then $5\Lambda(f_{a,b}) = -\#G_a^5 - 2\#G_a + 3\#H_a$;*
   (c) *if b is a primitive 3-rd root of unity, then $5\Lambda(f_{a,b}) = 2\#G_a^5 - \#G_a - \#H_a$.*

Now recall that the zeta function of a (smooth projective) curve C defined over $\mathbb{F}_q$ is

$$Z(C/\mathbb{F}_q; t) = \exp\left(\sum_{i=1}^{\infty} \frac{\#C(\mathbb{F}_{q^i})}{i} t^i\right) \ .$$

Weil proved that, for a curve of genus g, the zeta function $Z(C/\mathbb{F}_q; t)$ can be written as a rational function

$$Z(C/\mathbb{F}_q; t) = \frac{t^{2g}\chi(1/t)}{(1-t)(1-qt)} \ ,$$

where $\chi(t)$ is the characteristic polynomial of the Frobenius endomorphism of the Jacobian of C and that

$$\chi(t) = a_g t^g + \sum_{i=0}^{g-1} a_i (t^{2g-i} + q^{g-i} t^i) \ .$$

Table 7.3 – Meantimes needed to compute the number of points on G_a, H_a, G_a^5 and H_a^5

m	$\#G_a$	$\#H_a$	$\#G_a^5$	$\#H_a^5$	m	$\#G_a$	$\#H_a$	$\#G_a^5$	$\#H_a^5$
6	0.000	0.001	0.000	0.000	30	0.024	1.165	132.982	197.473
10	0.001	0.001	0.000	0.000	34	0.035	1.376	338.97	570.014
14	0.010	0.012	0.020	0.019	38	0.080	1.520	394.670	627.62
18	0.244	0.217	0.309	0.318	42	0.050	2.390	491.030	958.810
22	0.019	0.634	52.533	81.334	46	0.037	5.069	742.901	1111.722
26	0.021	0.850	82.884	143.275	50	0.042	7.814	1022.621	1428.279

In particular, the knowledge of $\chi(t)$ and its factorization over the complex numbers entails that of $\#C(\mathbb{F}_{q^i})$ for all $i \geq 1$. In particular, one has

$$\#C(\mathbb{F}_q) = q + 1 + a_1 \ .$$

Furthermore, the curves we defined are in fact *Artin–Schreier* curves, which are a special kind of imaginary hyperelliptic curves in even characteristic, and Denef and Vercauteren [79, 253] have shown that it is possible to efficiently compute their zeta functions.

Theorem 7.3.7 ([253, Theorem 4.3.1])**.** *Let C be an Artin–Schreier curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the zeta function of C in*

$$O(g^3 m^3 (g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

bit operations and $O(g^3 m^3)$ memory.

We can therefore compute the number of points of such curves in polynomial time and space in the size of the base field. It should also be remarked that the time and space complexities of the above algorithm are also polynomial in the genus of the curve.

If we fix a set $R \subset E$ of indices and suppose that the maximum index $r_{max} \in R$ is odd, then the genera of the curves H_a^5, G_a^5, H_a and G_a are respectively $\frac{5r_{max}+1}{2}$, $\frac{5r_{max}-1}{2}$, $\frac{r_{max}+1}{2}$ and $\frac{r_{max}-1}{2}$. Therefore, even though the overall time and space complexities in m of the point counting algorithm will not change, discarding the computation of the zeta function of the curve H_a^5 by using the reformulation of Theorem 7.3.6, rather than that of Theorem 7.3.5, will have a practical impact.

To illustrate this fact, we performed several simulations with Magma v2.18-2 [8]. The computations were performed on an Intel Core2 Quad CPU Q6600 cadenced at 2.40 GHz. The set R of indices used was $R = \{1, 3\}$ and ten couples of coefficients (a_1, a_3) were randomly generated in $\mathbb{F}_{2^m}^*$. The meantimes needed to compute the number of points on the curves G_a, H_a, G_a^5 and H_a^3 for integers $m \equiv 2 \pmod 4$ between 6 and 50 are presented in Table 7.3. It should be noted that Magma [8] actually uses a naive point counting algorithm for $m \leq 20$ and switches to the Vercauteren–Kedlaya algorithm for higher values. Nonetheless, the time needed for the naive method growing exponentially, it quickly becomes far less efficient than the Vercauteren–Kedlaya one, even for curves of high genera such as G_a^5 and H_a^5.

We now provide numerical evidence that the characterizations using hyperelliptic curves are more efficient than those involving exponential sums not only asymptotically, but also for practical values of m. Table 7.4 gives the meantimes needed to test the hyper-bentness of ten randomly chosen functions $f_{a,b}$ with $R = \{1, 3\}$ and $b = 1$ using Magma [8] implementations of Proposition 6.3.2 (denoted by Λ), Theorem 6.6.5 (denoted by T_1) and Theorem 7.3.6 (denoted by $\#G$) on the same hardware as above (for $m = 34$, only one couple was tested). Finally, a random

Table 7.4 – Meantimes needed to test the hyper-bentness of $f_{a,1}$

m	Λ	T_1	$\#G$	m	Λ	T_1	$\#G$
6	0.000	0.000	0.001	22	38.709	56.547	53.490
10	0.012	0.005	0.003	26	660.433	941.750	83.137
14	0.150	0.092	0.041	30	11271.549	16141.993	131.745
18	2.462	1.449	0.666	34	212549.620	277847.460	328.580

search on such functions using the latter test showed that the following couple (a_1, a_3):

$$\begin{aligned} a_1 = {} & x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{21} + x^{18} + \\ & x^{16} + x^{15} + x^{14} + x^{12} + x^6 + x^5 + x^3 + x^2 + x \ , \\ a_3 = {} & x^{29} + x^{28} + x^{25} + x^{24} + x^{23} + x^{20} + x^{16} + x^{15} + x^{14} + \\ & x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 \ , \end{aligned}$$

where $\mathbb{F}_{2^{30}}$ is represented as $\mathbb{F}_2[x]/(C_{30})$ with C_{30} the 30-th Conway polynomial, gives rise to a hyper-bent function $f_{a,1}$ in $n = 60$ inputs. Finding such a couple would have been quite difficult with a naive approach using exponential sums.

To conclude this section, we investigate the case where $R = \{1, 3\}$ and $a_1 = a_3 = a$ and b is a primitive element of $\mathbb{F}_4$ of trace zero. In this case, the functions of the Wang et al. family are of the form

$$f_{a,b} = \mathrm{Tr}_1^n \left(a \left(x^{3(2^m-1)} + x^{(2^m-1)} \right) \right) + \mathrm{Tr}_1^4 \left(b x^{\frac{2^n-1}{5}} \right) \ ,$$

and the associated condition for hyper-bentness is

$$T_1^5(g_a) = 2 \ ,$$

or equivalently

$$2\#G_a^5 - \#G_a - \#H_a = 5 \ .$$

For small values of m, numerical investigation pointed out that the associated value ν_a defined as

$$\nu_a = \frac{T_1^5(g_a) - 2}{10} + (-1)^{\frac{m-2}{4}} = \frac{2\#G_a^5 - \#G_a - \#H_a - 5}{20} + (-1)^{\frac{m-2}{4}}$$

takes even integer values with absolute value bounded by a given constant. For $m \in \{6, 10, 14, 18\}$, the constants were respectively 2, 12, 80 and 314. In particular, it is never equal to $(-1)^{\frac{m-2}{4}}$ and the associated family of Boolean functions contains no hyper-bent functions. Proving the above fact is therefore both of practical and theoretical interest.

7.3.4 Algorithmic generation of hyper-bent functions in the family $\mathcal{H}_n$ and hyperelliptic curves

Recall the fundamental connection between Boolean functions, exponential sums and hyperelliptic curves.

Proposition 7.3.8 ([101, Propositions 3.3 and 3.4])**.** *Let $\widetilde{g} : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $\widetilde{g}(0) = 0$ and g be the corresponding Boolean function $g = \mathrm{Tr}_1^m(\widetilde{g})$. Let G_g be the (affine) curve defined over $\mathbb{F}_{2^m}$ by*

$$G_g : y^2 + y = \widetilde{g}(x) \ ,$$

and H_g be the (affine) curve defined over $\mathbb{F}_{2^m}$ by

$$H_g : y^2 + xy = x + x^2\widetilde{g}(x) \ .$$

Then

$$\Xi(g) = \#G_g - 2^m \ ,$$
$$\Xi(\mathrm{Tr}_1^m(1/x) + g(x)) = \#H_g - 2^m + 1 \ .$$

We superscript the curves G_g and H_g by r to mean that the corresponding functions $\widetilde{g}$ and g are composed with D_r, i.e. $G_g^r = G_{g\circ D_r}$ and $H_g^r = H_{g\circ D_r}$.

Proposition 7.3.8 gives the following reformulation of Lemma 2.4.8 in terms of curves.

Corollary 7.3.9. *The notation is as in Proposition 7.3.8. Then*

$$T_i(g) = \frac{1}{2}\left((\#G_g - 2^m) + \chi(i)\,(\#H_g - 2^m + 1)\right) \ .$$

When applied to Corollary 2.4.6, we get the following interesting result about curves.

Corollary 7.3.10. *The notation is as in Proposition 7.3.8. Let moreover $1 \leq r \leq 2^n - 1$ be an integer such that $k = \gcd(r, 2^m - 1) = 1$. Then*

$$\#G_g^r + \#H_g^r = \#G_g + \#H_g \ .$$

In this subsection, we are interested in the algorithmic generation of hyper-bent functions in the family $\mathcal{H}_n$. Recall that a function $f_{a,b} \in \mathcal{H}_n$ is of the form

$$f_{a,b}(x) = \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^t\left(b x^{\frac{2^m+1}{\tau}(2^m-1)}\right) \ ,$$

and that it is hyper-bent if and only if the corresponding value $\Lambda(a,b) = \Lambda(f_{a,b}) = 1$.

We show how the results of Section 6.6 can be reformulated in terms of hyperelliptic curves. This was done for the Charpin–Gong family [170] (i.e. for the family $\mathcal{F}_n$), in the cases $\tau = 3$ [101] (i.e. for the family $\mathfrak{H}_n$) and $\tau = 5$ [102] (i.e. for the family of Wang et al.), leading in these three cases to both theoretical and practical improvements. In particular, hyper-bent functions were devised which could not have been generated by naive computation of exponential sums.

Here, we generalize these approaches, apply them to the families described in Section 6.6 and provide a complexity analysis of the corresponding tests for hyper-bentness. Furthermore, we study how the different available tests behave as τ grows and which one is the fastest for *explicit* generation of hyper-bent functions, that is for moderate values of m where the tests actually permit to generate hyper-bent functions through a random search on the coefficients a_r.

Before taking this quite algorithmic and practical point of view, let us mention that reformulating the previous characterizations in terms of number of points on hyperelliptic curves is also of high theoretical interest. The theory of algebraic curves is rich and can be applied to the study of hyper-bent function through such reformulations. For example, Lachaud and Wolfmann [156, Theorem 3.4] used the theory of elliptic curves to prove that Kloosterman sums take every value divisible by 4 within a given interval and in particular the value zero. A consequence of this result is the existence of hyper-bent monomial functions with the Dillon exponent for every extension degree m, a question which was left as an open problem by Dillon.

Characterizations in terms of hyperelliptic curves

1. The family $\mathcal{G}_n$

   To begin with, it should be remarked that Lisoněk criterion for the Charpin–Gong family $\mathcal{F}_n$ [170, Theorem 2] readily extends to the family $\mathcal{G}_n$. Applying Corollary 7.3.9 to Theorem 6.4.9 indeed yields a similar reformulation.

   Proposition 7.3.11. *The notation is as in Theorem 6.4.9. Then*

   $$\Lambda(a) = \#G_{g_a} - \#H_{g_a} \ .$$

2. The case $b = 1$

   In the case $b = 1$, we have different characterizations for the hyper-bentness of $f_{a,1}$. Indeed, $f_{a,1}$ lies not only in $\mathcal{H}_n$, but also in $\mathcal{G}_n \subsetneq \mathcal{H}_n$.

   In the formalism of Subsection 6.6.1, applying Corollary 7.3.9 to Proposition 6.6.1 yields the following reformulation which is nothing but a variation of Proposition 7.3.11.

   Proposition 7.3.12. *Let g'_a be the Boolean function defined on $\mathbb{F}_{2^m}$ as $g'_a(x) = g_a(x) + \mathrm{Tr}_1^m(D_s(x))$. Then*

   $$\Lambda(a,1) = \#G_{g'_a} - \#H_{g'_a} \ .$$

   Recall now that the additional trace term of $f_{a,1}$ involves the Dillon-like exponent $s(2^m-1)$ and that the extension degree m verifies $m \equiv o \pmod{2o}$ where $2o$ is the multiplicative order of 2 modulo $\tau = \frac{2^m+1}{s}$. In particular, τ divides 2^m+1 and is co-prime with 2^m-1, so that not only Corollary 7.3.9, but also Corollary 7.3.10, can be applied to Proposition 6.6.3. Doing so, we obtain two different reformulations.

   Proposition 7.3.13. *Suppose that $\tau = p^k$ is a prime power and that 2 is a primitive root modulo p^k. Then*

   $$\begin{aligned} p^k\Lambda(a,1) &= 2\left(\#G_{g_a}^{p^k} - \#H_{g_a}^{p^k}\right) - 2p\left(\#G_{g_a}^{p^{k-1}} - \#H_{g_a}^{p^{k-1}}\right) + p^k\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G_{g_a}^{p^k} - 4p\#G_{g_a}^{p^{k-1}} + (p^k+2p-2)\#G_{g_a} - (p^k-2p+2)\#H_{g_a} \ . \end{aligned}$$

3. The case $\tau = 3$

   For the record, we recall how Corollaries 7.3.9 and 7.3.10 apply to Theorem 6.6.4 in the case $\tau = 3$.

   Proposition 7.3.14. *Let $\tau = 3$ and $m \equiv 1 \pmod 2$. Then*

   (a) If $b = 1$, then

   $$\begin{aligned} 3\Lambda(a,b) &= 2\left(\#G_{g_a}^3 - \#H_{g_a}^3\right) - 3\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G_{g_a}^3 - 5\#G_{g_a} + \#H_{g_a} \ . \end{aligned}$$

   (b) If b is a primitive element of $\mathbb{F}_4$, then

   $$\begin{aligned} 3\Lambda(a,b) &= -\left(\#G_{g_a}^3 - \#H_{g_a}^3\right) \ , \\ &= -2\#G_{g_a}^3 + \#G_{g_a} + \#H_{g_a} \ . \end{aligned}$$

4. The case $\tau = 5$

   For the record, we recall how Corollaries 7.3.9 and 7.3.10 apply to Theorem 6.6.5 in the case $\tau = 5$.

   Proposition 7.3.15. *Let $\tau = 5$ and $m \equiv 2 \pmod 4$.*

   (a) If $b = 1$, then

   $$\begin{aligned} 5\Lambda(a,b) &= 2\left(\#G^5_{g_a} - \#H^5_{g_a}\right) - 5\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^5_{g_a} - 7\#G_{g_a} + 3\#H_{g_a} \ . \end{aligned}$$

   (b) If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}^4_1(b) = 0$, i.e. with minimal polynomial $x^4 + x + 1$, then

   $$\begin{aligned} 5\Lambda(a,b) &= \#G^5_{g_a} - \#H^5_{g_a} \ , \\ &= 2\#G^5_{g_a} - \#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

   (c) Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$.

   i. If b is a primitive 3-rd root of unity, i.e. with minimal polynomial $x^2 + x + 1$, then

   $$\begin{aligned} 5\Lambda(a,b) &= \#G^5_{g_a} - \#H^5_{g_a} \ , \\ &= 2\#G^5_{g_a} - \#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

   ii. If b is a primitive 5-th root of unity, i.e. with minimal polynomial $x^4+x^3+x^2+x+1$, then

   $$\begin{aligned} 10\Lambda(a,b) &= -\left(\#G^5_{g_a} - \#H^5_{g_a}\right) - \left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -2\#G^5_{g_a} - 4\#G_{g_a} + 6\#H_{g_a} \ . \end{aligned}$$

   iii. If b is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}^4_1(b) = 1$, i.e. with minimal polynomial $x^4 + x^3 + 1$, then

   $$\begin{aligned} 10\Lambda(a,b) &= -3\left(\#G^5_{g_a} - \#H^5_{g_a}\right) + 5\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -6\#G^5_{g_a} + 8\#G_{g_a} - 2\#H_{g_a} \ . \end{aligned}$$

5. The case $\tau = 9$

   Applying Corollaries 7.3.9 and 7.3.10 to Theorem 6.6.6 gives the following reformulations for $\tau = 9$.

   Proposition 7.3.16. *Let $\tau = 9$ and $m \equiv 3 \pmod 6$.*

   (a) If $b = 1$, then

   $$\begin{aligned} 9\Lambda(a,b) &= 2\left(\#G^9_{g_a} - \#H^9_{g_a}\right) - 6\left(\#G^3_{g_a} - \#H^3_{g_a}\right) + 9\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^9_{g_a} - 12\#G^3_{g_a} + 13\#G_{g_a} - 5\#H_{g_a} \ . \end{aligned}$$

   (b) If b is a primitive 3-rd root of unity, then

   $$\begin{aligned} 9\Lambda(a,b) &= -\left(\#G^9_{g_a} - \#H^9_{g_a}\right) - 3\left(\#G^3_{g_a} - \#H^3_{g_a}\right) + 9\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -2\#G^9_{g_a} - 6\#G^3_{g_a} + 13\#G_{g_a} - 5\#H_{g_a} \ . \end{aligned}$$

(c) Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{3}}}$ *and* $\frac{m}{3} \not\equiv 0 \pmod 3$.

i. If b *is a primitive* 7*-th root of unity with minimal polynomial* x^3+x+1 *or a primitive element with minimal polynomial* x^6+x+1*, then*

$$\begin{aligned} 9\Lambda(a,b) &= 4\left(\#G^3_{g_a} - \#H^3_{g_a}\right) - 3\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 8\#G^3_{g_a} - 7\#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

ii. If b *is a primitive* 7*-th root of unity with minimal polynomial* x^3+x^2+1 *or a* 21*-st root of unity with minimal polynomial* $x^6+x^4+x^2+x+1$*, then*

$$\begin{aligned} 9\Lambda(a,b) &= 2\left(\#G^9_{g_a} - \#H^9_{g_a}\right) - 2\left(\#G^3_{g_a} - \#H^3_{g_a}\right) - 3\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^9_{g_a} - 4\#G^3_{g_a} - 3\#G_{g_a} + 3\#H_{g_a} \ . \end{aligned}$$

iii. If b *is a primitive* 9*-th root of unity with minimal polynomial* x^6+x^3+1*, then*

$$\begin{aligned} 9\Lambda(a,b) &= 2\left(\#G^3_{g_a} - \#H^3_{g_a}\right) + 3\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^3_{g_a} + \#G_{g_a} - 5\#H_{g_a} \ . \end{aligned}$$

iv. If b *is a primitive* 21*-st root of unity with minimal polynomial* $x^6+x^5+x^4+x^2+1$*, or a primitive element with minimal polynomial* $x^6+x^5+x^3+x^2+1$ *or* $x^6+x^5+x^4+x+1$*, then*

$$\begin{aligned} 9\Lambda(a,b) &= -\left(\#G^9_{g_a} - \#H^9_{g_a}\right) + \left(\#G^3_{g_a} - \#H^3_{g_a}\right) - 3\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -2\#G^9_{g_a} + 2\#G^3_{g_a} - 3\#G_{g_a} + 3\#H_{g_a} \ . \end{aligned}$$

v. If b *is a primitive element with minimal polynomial* $x^6+x^4+x^3+x+1$*, then*

$$\begin{aligned} 9\Lambda(a,b) &= 2\left(\#G^9_{g_a} - \#H^9_{g_a}\right) - 4\left(\#G^3_{g_a} - \#H^3_{g_a}\right) + 3\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^9_{g_a} - 8\#G^3_{g_a} + 5\#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

vi. If b *is a primitive element with minimal polynomial* x^6+x^5+1 *or* $x^6+x^5+x^2+x+1$*, then*

$$\begin{aligned} 9\Lambda(a,b) &= -\left(\#G^9_{g_a} - \#H^9_{g_a}\right) - \left(\#G^3_{g_a} - \#H^3_{g_a}\right) + 3\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -2\#G^9_{g_a} - 2\#G^3_{g_a} + 5\#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

6. The case $\tau = 11$

Applying Corollaries 7.3.9 and 7.3.10 to Theorem 6.6.7 gives the following reformulations for $\tau = 11$.

Proposition 7.3.17. *Let* $\tau = 11$ *and* $m \equiv 5 \pmod{10}$.

(a) If $b = 1$*, then*

$$\begin{aligned} 11\Lambda(a,b) &= 2\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) - 11\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^{11}_{g_a} - 13\#G_{g_a} + 9\#H_{g_a} \ . \end{aligned}$$

(b) If b *is a primitive* 3*-rd root of unity, a* 341*-st root of unity with minimal polynomial* $x^{10}+x^9+x^8+x^3+x^2+x+1$*, or a primitive element with minimal polynomial* $x^{10}+x^9+x^8+x^4+x^3+x^2+1$ *or* $x^{10}+x^9+x^8+x^6+x^5+x+1$*, then*

$$\begin{aligned} 11\Lambda(a,b) &= -\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) \ , \\ &= -2\#G^{11}_{g_a} + \#G_{g_a} + \#H_{g_a} \ . \end{aligned}$$

7. The case $\tau = 13$

Applying Corollaries 7.3.9 and 7.3.10 to Theorem 6.6.8 gives the following reformulations for $\tau = 13$.

Proposition 7.3.18. *Let $\tau = 13$ and $m \equiv 6 \pmod{12}$.*

(a) If $b = 1$, then

$$\begin{aligned} 13\Lambda(a,b) &= 2\left(\#G_{g_a}^{13} - \#H_{g_a}^{13}\right) - 13\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G_{g_a}^{13} - 15\#G_{g_a} + 11\#H_{g_a} \ . \end{aligned}$$

(b) If b is a primitive 15-th root of unity with minimal polynomial $x^4 + x + 1$, a primitive 819-th root of unity with minimal polynomial $x^{12} + x^9 + x^8 + x^5 + x^4 + x + 1$, a primitive 1365-th root of unity with minimal polynomial $x^{12} + x^9 + x^5 + x^2 + 1$, or a primitive element with minimal polynomial $x^{12} + x^9 + x^5 + x^4 + x^2 + x + 1$, $x^{12} + x^9 + x^8 + x^5 + 1$ or $x^{12} + x^9 + x^8 + x^6 + x^3 + x^2 + 1$, then

$$\begin{aligned} 13\Lambda(a,b) &= \#G_{g_a}^{13} - \#H_{g_a}^{13} \ , \\ &= 2\#G_{g_a}^{13} - \#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

8. The case $\tau = 17$

Applying Corollaries 7.3.9 and 7.3.10 to Theorem 6.6.9 gives the following reformulations for $\tau = 17$.

Proposition 7.3.19. *Let $\tau = 17$ and $m \equiv 4 \pmod{8}$. Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$.*

(a) If b is a primitive element with minimal polynomial $x^8 + x^6 + x^5 + x + 1$ or $x^8 + x^6 + x^5 + x^2 + 1$, then

$$\begin{aligned} 17\Lambda(a,b) &= \#G_{g_a}^{17} - \#H_{g_a}^{17} \ , \\ &= 2\#G_{g_a}^{17} - \#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

(b) Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{4}}}$.

i. If b is a primitive 15-th root of unity with minimal polynomial $x^4 + x + 1$, a primitive 17-th root of unity with minimal polynomial $x^8 + x^5 + x^4 + x^3 + 1$, or a primitive element with minimal polynomial $x^8 + x^5 + x^3 + x^2 + 1$, then

$$\begin{aligned} 17\Lambda(a,b) &= \#G_{g_a}^{17} - \#H_{g_a}^{17} \ , \\ &= 2\#G_{g_a}^{17} - \#G_{g_a} - \#H_{g_a} \ . \end{aligned}$$

ii. If b is a 51-st root of unity with minimal polynomial $x^8 + x^4 + x^3 + x + 1$, then

$$\begin{aligned} 34\Lambda(a,b) &= 3\left(\#G_{g_a}^{17} - \#H_{g_a}^{17}\right) - 17\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 6\#G_{g_a}^{17} - 20\#G_{g_a} + 14\#H_{g_a} \ . \end{aligned}$$

9. The case $\tau = 33$

Applying Corollaries 7.3.9 and 7.3.10 to Theorem 6.6.10 gives the following reformulations for $\tau = 33$.

Proposition 7.3.20. *Let $\tau = 33$ and $m \equiv 5 \pmod{10}$. Suppose moreover that $a_r \in \mathbb{F}_{2^{\frac{m}{5}}}$ and $\frac{m}{5} \not\equiv 0 \pmod 5$.*

(a) If b is a primitive 31-st root of unity with minimal polynomial x^5+x^2+1, or a primitive 341-st root of unity with minimal polynomial $x^{10}+x^8+x^4+x^3+x^2+x+1$, then

$$\begin{aligned} 165\Lambda(a,b) &= 4\left(\#G^{33}_{g_a} - \#H^{33}_{g_a}\right) + 12\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) \\ &\quad - 44\left(\#G^{3}_{g_a} - \#H^{3}_{g_a}\right) + 33\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 8\#G^{33}_{g_a} + 24\#G^{11}_{g_a} - 88\#G^{3}_{g_a} + 61\#G_{g_a} - 5\#H_{g_a} \ . \end{aligned}$$

(b) If b is a primitive 31-st root of unity with minimal polynomial x^5+x^3+1, then

$$\begin{aligned} 165\Lambda(a,b) &= -4\left(\#G^{33}_{g_a} - \#H^{33}_{g_a}\right) + 24\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) \\ &\quad + 44\left(\#G^{3}_{g_a} - \#H^{3}_{g_a}\right) - 99\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -8\#G^{33}_{g_a} + 48\#G^{11}_{g_a} + 88\#G^{3}_{g_a} - 163\#G_{g_a} + 35\#H_{g_a} \ . \end{aligned}$$

(c) If b is a primitive 31-st root of unity with minimal polynomial $x^5+x^3+x^2+x+1$, a primitive 93-rd root of unity with minimal polynomial $x^{10}+x^8+x^3+x+1$, a primitive 341-st root of unity with minimal polynomial $x^{10}+x^8+x^7+x^5+x^3+x+1$, or a primitive element with minimal polynomial $x^{10}+x^7+1$, $x^{10}+x^7+x^6+x^4+x^2+x+1$ or $x^{10}+x^8+x^7+x^5+1$, then

$$\begin{aligned} 165\Lambda(a,b) &= 12\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) + 33\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 24\#G^{11}_{g_a} + 21\#G_{g_a} - 45\#H_{g_a} \ . \end{aligned}$$

(d) If b is a primitive 93-rd root of unity with minimal polynomial $x^{10}+x^5+x^4+x^2+1$, or a primitive element with minimal polynomial $x^{10}+x^6+x^5+x^3+x^2+x+1$ or $x^{10}+x^8+x^5+x^4+x^3+x^2+1$, then

$$\begin{aligned} 165\Lambda(a,b) &= -2\left(\#G^{33}_{g_a} - \#H^{33}_{g_a}\right) + 18\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) \\ &\quad + 22\left(\#G^{3}_{g_a} - \#H^{3}_{g_a}\right) - 33\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -4\#G^{33}_{g_a} + 36\#G^{11}_{g_a} + 44\#G^{3}_{g_a} - 71\#G_{g_a} - 5\#H_{g_a} \ . \end{aligned}$$

(e) If b is a primitive 93-rd root of unity with minimal polynomial $x^{10}+x^8+x^6+x^5+1$, then

$$\begin{aligned} 165\Lambda(a,b) &= 2\left(\#G^{33}_{g_a} - \#H^{33}_{g_a}\right) + 18\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) \\ &\quad - 22\left(\#G^{3}_{g_a} - \#H^{3}_{g_a}\right) - 33\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^{33}_{g_a} + 36\#G^{11}_{g_a} - 44\#G^{3}_{g_a} - 31\#G_{g_a} + 35\#H_{g_a} \ . \end{aligned}$$

(f) If b is a primitive 341-st root of unity with minimal polynomial $x^{10}+x^3+x^2+x+1$ or $x^{10}+x^7+x^4+x^3+1$, then

$$\begin{aligned} 165\Lambda(a,b) &= -4\left(\#G^{33}_{g_a} - \#H^{33}_{g_a}\right) + 18\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) \\ &\quad + 44\left(\#G^{3}_{g_a} - \#H^{3}_{g_a}\right) - 33\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= -8\#G^{33}_{g_a} + 36\#G^{11}_{g_a} + 88\#G^{3}_{g_a} - 91\#G_{g_a} - 25\#H_{g_a} \ . \end{aligned}$$

(g) If b is a primitive 341-st root of unity with minimal polynomial $x^{10}+x^6+x^2+x+1$, or a primitive element with minimal polynomial $x^{10}+x^7+x^3+x+1$, then

$$\begin{aligned} 165\Lambda(a,b) &= 18\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) - 33\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 36\#G^{11}_{g_a} - 51\#G_{g_a} + 15\#H_{g_a} \ . \end{aligned}$$

(h) If b is a primitive element with minimal polynomial $x^{10}+x^7+x^6+x^5+x^4+x+1$ or $x^{10}+x^7+x^6+x^5+x^4+x^3+x^2+x+1$, then

$$\begin{aligned} 165\Lambda(a,b) &= 2\left(\#G^{33}_{g_a} - \#H^{33}_{g_a}\right) + 12\left(\#G^{11}_{g_a} - \#H^{11}_{g_a}\right) \\ &\quad - 22\left(\#G^{3}_{g_a} - \#H^{3}_{g_a}\right) + 33\left(\#G_{g_a} - \#H_{g_a}\right) \ , \\ &= 4\#G^{33}_{g_a} + 24\#G^{11}_{g_a} - 44\#G^{3}_{g_a} + 41\#G_{g_a} - 25\#H_{g_a} \ . \end{aligned}$$

Asymptotic complexities

Asymptotically, to test the hyper-bentness of any function in the family $\mathcal{H}_n$ through a naive computation of $\Lambda(f_{a,b})$, that is a partial exponential sum over $U \subset \mathbb{F}_{2^n}$, one has to compute $\#U = 2^m + 1$ summands. For each summand, the computation is dominated by the cost of an exponentiation with an arbitrary large exponent because r_{max}, the maximal index in R, grows exponentially with m. Therefore, the total computation has a time complexity of $O(2^m m^{2+\epsilon})$ and a space complexity of $O(m)$. Using the characterizations given in Section 6.6 yields similar complexities, the only notable difference being that the finite field arithmetic occurs in $\mathbb{F}_{2^m}$ rather than $\mathbb{F}_{2^n}$.

As far as the characterizations of the previous subsection are concerned, the situation is not better if one wants to test any function in the family $\mathcal{H}_n$. Indeed, the time and space complexities of the point counting algorithms described in Theorems 7.1.7 and 7.1.8 are polynomial in the genus of the curve, and so are in the maximal index $r_{max} \in R$.

More precisely, we can suppose that r_{max} is odd, so that it is as small as possible and the curves involved in the characterizations are Artin–Schreier curves. Then, for any odd integer $l \geq 1$, the curves $G^l_{g_a}$ and $H^l_{g_a}$ are of genera respectively $\frac{lr_{max}-1}{2}$ and $\frac{lr_{max}+1}{2}$. Therefore, for a fixed τ and a family $\mathcal{T}_n$ of Boolean functions among the ones studied in the previous subsection (*e.g.* the family $\mathcal{T}_n = \{f_{a,b} \in \mathcal{H}_n \mid \tau = 9$ and b is a 3-rd root of unity$\}$), one gets the following theorem.

Theorem 7.3.21. *For a fixed τ, the hyper-bentness of $f_{a,b} \in \mathcal{T}_n$ defined over $\mathbb{F}_{2^n}$, where $\mathcal{T}_n$ is a family defined as above, can be checked in*

$$O(r_{max}^{7.376} m^2 + r_{max}^{3.376} m^{2.667})$$

bit operations and $O(r_{max}^5 m^2 + r_{max}^3 m^{2.5})$ memory.

As the maximal index r_{max} grows exponentially with m, these complexities are still exponential in the extension degree m. Nonetheless, it is customary in cryptography to restrict to functions of a given form, that is to fix the set R. In this case, r_{max} does not grow with m. On the one hand, the time complexities of the two naive approaches fall to $O(2^m m^{1+\epsilon})$, the computation of one term being dominated by the cost of a multiplication, and so are still exponential. On the other hand, the time and space complexities of the tests involving hyperelliptic curves become polynomial in m, except for Proposition 7.3.13.

Theorem 7.3.22. *For a fixed τ and a fixed R, the hyper-bentness of $f_{a,b} \in \mathcal{T}_n$ defined over $\mathbb{F}_{2^n}$ can be checked in polynomial time and space.*

To conclude, it should be remarked that, except for a few exceptions, all the characterizations devised above include a curve of genus $\frac{\tau r_{max}-1}{2}$. Therefore, the time and space complexities of the tests involving hyperelliptic curves will be polynomial in τ. For example, Proposition 7.3.13, where $b = 1$ and $\tau = p^k$ is a prime power for which 2 is primitive root, yields infinite families of τ for which the corresponding characterization involves a curve of genus exactly $\frac{\tau r_{max}-1}{2}$ as follows: choose p such that 2 is a primitive root modulo p^2, *e.g.* $p = 3$, and consider the family $\left\{p^k\right\}_{k=2}^{+\infty}$.

Experimental results

Although it has been demonstrated that characterizations involving hyperelliptic curves not only yield asymptotically faster algorithms, but also more practical ones for moderate values of m especially interesting in cryptography ([170] for the family $\mathcal{F}_n$, [101] for $\tau = 3$ and [102, Table 2] for $\tau = 5$) it is not clear that this remains true as τ grows.

• Naive computations:

Let us first compare the two characterizations of hyper-bentness involving exponential sums that we described in the previous sections, namely the characterization of Proposition 6.4.2 involving $\Lambda(a, b)$ and the characterizations of Section 6.6 involving $T_1(g_a \circ D_r)$. Although the arithmetic takes place in $\mathbb{F}_{2^n}$ for the former one, whereas it takes place in $\mathbb{F}_{2^m}$ for the latter ones, this is quite negligible for the small values of m which can be attained in practice. Moreover, the first criterion involves the computation of only one exponential sums over the set U of size $\#U = 2^m + 1$, whereas the second ones involve the computations of several exponential over the set $\mathcal{T}_1$ of size $\#\mathcal{T}_1 = 2^{m-1}$. For example, the characterization of Proposition 6.6.3, involves three different exponential sums, and the characterizations of Theorem 6.6.10 up to four different ones. Plus, the computation of g_a and its compositions with Dickson polynomials can be more complex than that of $f_{a,b}$.

To confirm these facts and compare the time needed by a direct computation of $\Lambda(a, b)$ as suggested by Proposition 6.4.2 and by a computation based on Proposition 6.6.3 and exponential sums over $\mathcal{T}_1$, we performed different experiments with version 2.18-5 of the Magma software [8] running on an Intel(R) Xeon(R) X5650 CPU cadenced at 2.67GHz for $R = \{1\}$, a_1 randomly chosen in $\mathbb{F}_{2^m}$, $b = 1$, and different values of τ and m. Given a value of τ, some restrictions lie on the extension degree m for the expression of $f_{a,b}$, i.e. m should divide $2^m + 1$. Therefore, for unsuitable values of m, the time needed for a direct computation of $\Lambda(a, b)$ were extrapolated. Nevertheless, the expression of $\Lambda(a, b)$ in Proposition 6.6.3 involving exponential sums on $\mathcal{T}_1$ can always be computed, even though $\Lambda(a, b)$ itself is not well defined in this case. Thus, for Proposition 6.6.3 the computations were performed for every extension degree. The results of these experiments are summarized in Figures 7.1 and 7.2 where the time needed to compute $\Lambda(a, b)$ directly or through Proposition 6.6.3 for m between 20 and 30 and $\tau = 3$ and 5 are depicted. Similar results can be observed for higher values of τ, *e.g.* 9, 11 and so on; that is, computing directly $\Lambda(a, b)$ is faster than computing it through the expression given in Proposition 6.6.3.

Finally, it should be noted that the characterization of Proposition 6.4.2, not only covers the family $\mathcal{H}_n$, but the complete family $\mathcal{F}_n$, that is all Boolean functions with Dillon-like exponents without any restriction on the coefficients $a_r \in \mathbb{F}_{2^m}$, nor on the sizes of the cyclotomic cosets of the exponents r.

• Using hyperelliptic curves

Now, the time needed by the two above methods grows exponentially with m, whereas the time needed by methods involving hyperelliptic curves will only grow polynomially for a fixed set R. Nonetheless, the constants involved are much larger for the latter methods than for the

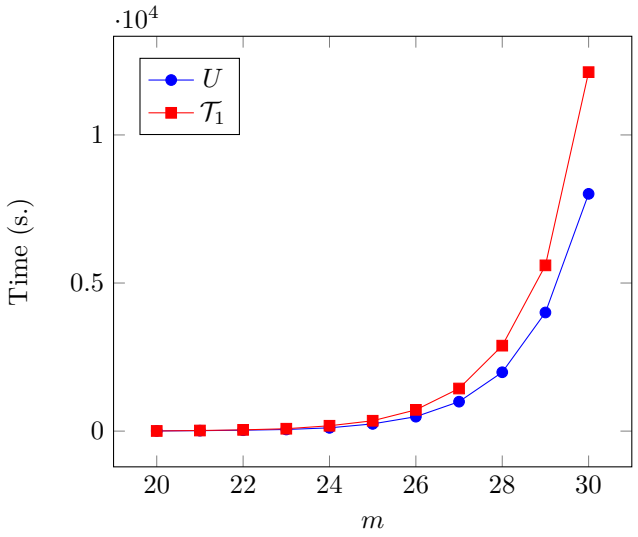

Figure 7.1 – Computation of $\Lambda(a, b)$ by summation over U and $\mathcal{T}_1$ for $\tau = 3$

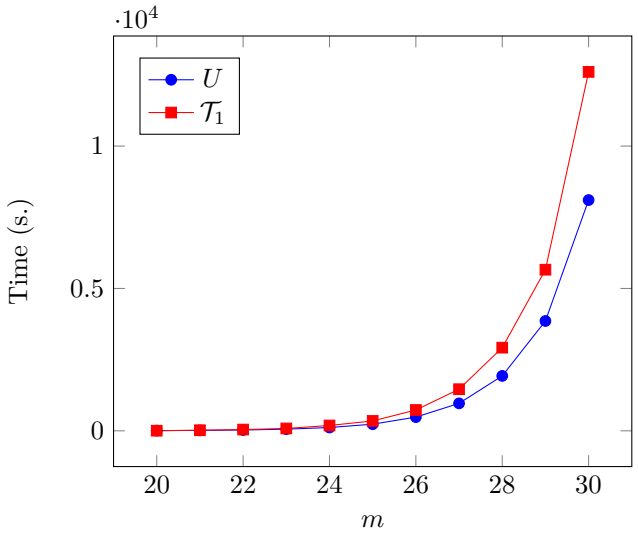

Figure 7.2 – Computation of $\Lambda(a, b)$ by summation over U and $\mathcal{T}_1$ for $\tau = 5$

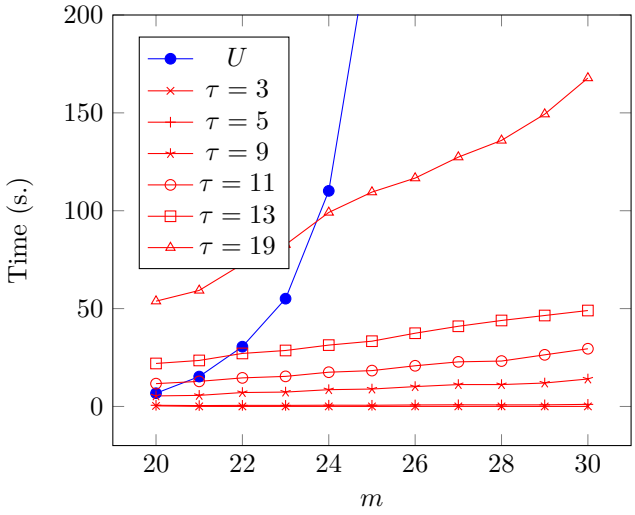

Figure 7.3 – Computation of $\Lambda(a, b)$ by summation over U and using hyperelliptic curves for $R = \{1\}$

former. Therefore, from a practical point of view, such methods are useless if they become more efficient for too large values of m.

Using the same setup as above, we compared the time needed to compute $\Lambda(a, b)$ directly and through the expression given in Proposition 7.3.13. Note that the Magma software uses a naive method to compute the number of points on a hyperelliptic curves of genus $g \geq 2$ for $m < 20$ and the Denef–Vercauteren algorithm from $m = 20$ onward. It also implements specialized point counting algorithms for elliptic curves and hyperelliptic curves of genus 2. As above, the definition of $f_{a,b}$ only makes sense for some extension degrees m, whereas the expression given by Proposition 7.3.13 always does. Therefore, timings using hyperelliptic curves where generated for every extension degrees between 20 and 30, even though the correspondence with $\Lambda(a, b)$ is not always valid. Moreover, the aforementioned computations for different values of τ showed that the time needed for a direct computation of $\Lambda(a, b)$ depends on τ in a negligible way. Hence, we only include timings of such a computation for a given value of τ chosen to be $\tau = 3$. Figure 7.3 gives timings for $R = 1$, that is for binomial functions, for different values of τ, whereas Figure 7.4 gives similar timings for $R = 1, 3$, that is for trinomial functions.

For $\tau = 3$ and 5, as was already shown in previous works [170, 101**?**], reformulations in terms of hyperelliptic curves yield non-negligible improvements, even for moderate values of m, when $R = \{1\}$ and $R = \{1, 3\}$ are considered. Indeed, such reformulations allow to generate hyper-bent functions which could not have been generated using more naive methods. For $R = \{1\}$, that is for the simplest binomial functions, Figure 7.3 suggests that this remains true for a few additional values of τ. This fact is confirmed by examples of hyper-bent functions given in Subsection 7.3.4.

On the contrary, Figure 7.4 shows that for trinomial functions with $R = \{1, 3\}$ and τ greater than 5, the crossover happens at extension degrees m for which testing hyper-bentness with a naive method, and using hyperelliptic curves, takes several hundreds of seconds. In particular, it seems hopeless to generate additional hyper-bent trinomials using tests based on hyperelliptic curves.

Nonetheless, the current Magma implementation of point counting over finite fields of even characteristic for hyperelliptic curves is limited to the Denef–Vercauteren algorithm. Algorithms

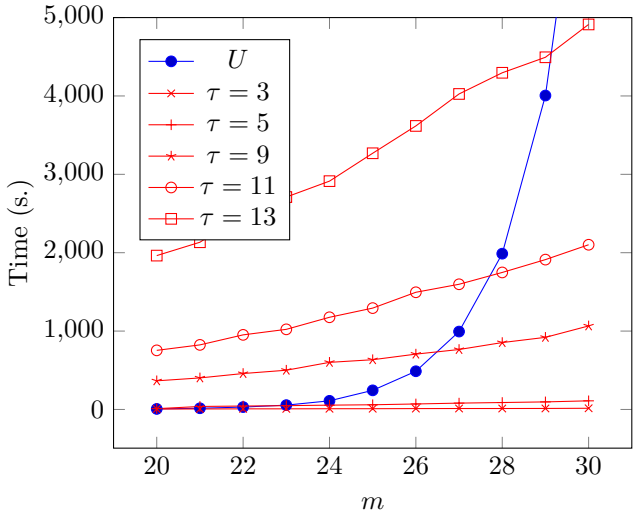

Figure 7.4 – Computation of $\Lambda(a, b)$ by summation over U and using hyperelliptic curves for $R = \{1, 3\}$

based on deformation theory are limited to odd characteristic. An efficient implementation of such algorithms in even characteristic should provide practical improvements, especially together with the possibility to count points on m different curves at a time with no runtime overhead by implementing multipoint evaluation as described by Hubrechts [135]. Furthermore, all the algorithms mentioned previously were designed not only to compute the number of rational points of a curve over its base field, but its complete zeta function, which is loosely equivalent to the knowledge of the number of points of the curve over the first g extension of the base field if the curve has genus g. Specializing these algorithms by lowering the needed precision during the computations to only compute the number of points of the curve over the base field, that is the trace term of the zeta function, should provide both better asymptotic complexities and practical improvements to the runtime.

• Examples of hyper-bent functions

To conclude this subsection, we provide some tuples of coefficients $(a_r)_{r\in R}$ corresponding to hyper-bent functions for different values of τ and b. They were generated through a random search, using the different characterizations proposed in this note. To describe the coefficients a_r, the finite field $\mathbb{F}_{2^m}$ is always represented as $\mathbb{F}_2[x]/(C_m(x))$ where $C_m(x)$ is the m-th Conway polynomial. Furthermore, recall that, although the coefficients a_r live in $\mathbb{F}_{2^m}$, the corresponding Boolean function $f_{a,b}$ is defined over $\mathbb{F}_{2^n}$ where $n = 2m$.

For example, when $b = 1$, we found that the function $f_{a,1}$ is hyper-bent if:

1. $\tau = 3$, $m = 33$, $a_1 = x^{32}+x^{28}+x^{27}+x^{25}+x^{24}+x^{20}+x^{19}+x^{14}+x^{13}+x^9+x^5+x^4+x^2+1$;
2. $\tau = 5$, $m = 34$, $a_1 = x^{33}+x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{23}+x^{22}+x^{20}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^2+1$;
3. $\tau = 5$, $m = 34$, $a_1 = x^{33}+x^{32}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{22}+x^{20}+x^{19}+x^{18}+x^{17}+x^{11}+x^9+x^6+x^3+x^2$, $a_3 = x^{33}+x^{31}+x^{29}+x^{28}+x^{25}+x^{23}+x^{22}+x^{18}+x^{17}+x^{16}+x^{14}+x^8+x^5+x^4+x^2$;
4. $\tau = 9$, $m = 21$, $a_1 = x^{20}+x^{17}+x^{15}+x^{14}+x^{10}+x^9+x^6+x^4+x^2+x$;

5. $\tau = 9$, $m = 21$, $a_1 = x^{18}+x^{17}+x^{12}+x^{11}+x^5+x^3+x+1$, $a_3 = x^{19}+x^{18}+x^{14}+x^8+x^7+x^4+1$;

6. $\tau = 9$, $m = 27$, $a_1 = x^{26} + x^{25} + x^{23} + x^{22} + x^{20} + x^{16} + x^9 + x^6$;

7. $\tau = 11$, $m = 15$, $a_1 = x^{15338}$;

8. $\tau = 11$, $m = 15$, $a_1 = x^{1066}$, $a_3 = x^{19316}$;

9. $\tau = 11$, $m = 25$, $a_1 = x^{24} + x^{22} + x^{17} + x^{13} + x^{11} + x^7 + x^5$;

10. $\tau = 13$, $m = 18$, $a_1 = x^{253630}$;

11. $\tau = 13$, $m = 18$, $a_1 = x^{247490}$, $a_3 = x^{216257}$;

12. $\tau = 13$, $m = 30$, $a_1 = x^{29} + x^{28} + x^{24} + x^{22} + x^{18} + x^{17} + x^{15} + x^6 + x^5 + x^3$.

For $b \neq 1$, here follow some examples of hyper-bent functions $f_{a,b}$:

1. $\tau = 3$, $m = 29$, $a_1 = x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{17} + x^{16} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^3$, b a primitive element of $\mathbb{F}_4$;

2. $\tau = 3$, $m = 33$, $a_1 = x^{29} + x^{26} + x^{24} + x^{23} + x^{20} + x^{18} + x^{17} + x^{16} + x^{15} + x^9 + x^8 + x^7 + x^6$, b a primitive element of $\mathbb{F}_4$;

3. $\tau = 5$, $m = 30$, $a_1 = x^{29} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{11} + x^{10} + x^9 + x^6 + x^5 + x^3 + x + 1$, b a primitive element of $\mathbb{F}_{16}$ with trace 0;

4. $\tau = 5$, $m = 34$, $a_1 = x^{33} + x^{29} + x^{25} + x^{23} + x^{22} + x^{21} + x^{20} + x^{16} + x^{15} + x^{14} + x^{11} + x^8 + x^6 + x^5 + x^4 + x^3$, b a primitive element of $\mathbb{F}_{16}$ with trace 0;

5. $\tau = 9$, $m = 21$, $a_1 = x^{20} + x^{19} + x^{17} + x^{15} + x^{14} + x^{13} + x^9 + x^8 + x^7 + x^4 + x^2 + 1$, b a primitive 3-rd root of unity;

6. $\tau = 9$, $m = 27$, $a_1 = x^{25} + x^{23} + x^{22} + x^{20} + x^{19} + x^{18} + x^{17} + x^{15} + x^{10} + x^9 + x^7 + x^6 + x^3$, b a primitive 3-rd root of unity;

7. $\tau = 11$, $m = 25$, $a_1 = x^{24} + x^{22} + x^{21} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^6 + x^3 + x^2$, b a primitive 3-rd root of unity;

8. $\tau = 13$, $m = 18$, $a_1 = x^{166827}$, b a primitive 15-th root of unity with minimal polynomial $x^4 + x + 1$;

9. $\tau = 13$, $m = 30$, $a_1 = x^{26} + x^{23} + x^{22} + x^{21} + x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^9 + x^6 + x$, b a primitive 15-th root of unity with minimal polynomial $x^4 + x + 1$.

Not only show the above examples the usefulness of our approach for explicit generation of hyper-bent functions, but also that the families of Boolean functions we consider actually contain hyper-bent functions.

7.4 Values of binary Kloosterman sums: some methods

7.4.1 Divisibility of binary Kloosterman sums

Classical results

Because of their cryptographic interest, divisibility properties of Kloosterman sums have been studied in several recent papers. A nice overview of such results can be found in the Ph.D. thesis of Moloney [207]. Here we cite a few of them which we will explicitly use in search algorithms for binary Kloosterman sums with specific values, especially the values 0 and 4.

Recall that Proposition 2.2.2 states in particular that binary Kloosterman sums are always divisible by 4. Afterwards, several papers studied divisibility properties of binary Kloosterman sums by multiples of 4 and other integers.

The following result was first proved by Helleseth and Zinoviev [128] and classifies the values of $K_m(a)$ modulo 8 according to the value of the absolute trace of a.

Proposition 7.4.1 ([128]). *Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}$. Then $K_m(a) \equiv 0 \pmod 8$ if and only if $\mathrm{Tr}_1^m(a) = 0$.*

In the same article, they gave the following sufficient conditions to get certain values of $K_m(a)$ modulo 3.

Proposition 7.4.2 ([128]). *Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}^*$. Suppose that there exists $t \in \mathbb{F}_{2^m}^*$ such that $a = t^4 + t^3$.*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$.*
- *If m is even, then $K_m(a) \equiv 0 \pmod 3$ if $\mathrm{Tr}_1^m(t) = 0$ and $K_m(a) \equiv -1 \pmod 3$ if $\mathrm{Tr}_1^m(t) = 1$.*

Furthermore, Charpin, Helleseth and Zinoviev [61] gave additional results about values of $K_m(a)$ modulo 3.

Proposition 7.4.3 ([61]). *Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}^*$. Then we have:*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 0$. This is equivalent to $a = \frac{b}{(1+b)^4}$ for some $b \in \mathbb{F}_{2^m}^*$.*
- *If m is even, then $K_m(a) \equiv 1 \pmod 3$ if and only if $a = b^3$ for some b such that $\mathrm{Tr}_2^m(b) \neq 0$.*

Further divisibility results exist and could be used to further refine the tests proposed in this chapter. For example, results up to 64 can be found in a paper of Göloğlu, McGuire and Moloney [119], and results up to 256 in an even more recent paper of Göloğlu, Lisoněk, McGuire and Moloney [118].

Most of these results about divisibility were first proved studying the link between exponential sums and coset weight distribution [128, 61]. However some of them can be proved in a completely different manner as we show in the next subsection.

Using torsion of elliptic curves

Theorem 7.2.1 giving the value of $K_m(a)$ as the cardinality of an elliptic curve can indeed be used to deduce divisibility properties of Kloosterman sums from the rich theory of elliptic curves. We recall that the quadratic twist of the ordinary elliptic curve E_a that we denote by $\widetilde{E}_a$ is given by the Weierstraß equation

$$\widetilde{E}_a : y^2 + xy = x^3 + bx^2 + a \ ,$$

where $b \in \mathbb{F}_{2^m}$ has absolute trace 1; it has cardinality:

$$\#\widetilde{E}_a = 2^m + 2 - K_m(a) \ .$$

First of all, we recall a proof of the divisibility by 4 stated in Proposition **??** as it can be found for example in the preprint of Ahmadi and Granger [1]. For $m \geq 3$, $K_m(a) \equiv \#E_a \pmod 4$, so $K_m(a) \equiv 0 \pmod 4$ if and only if $\#E_a \equiv 0 \pmod 4$. This is equivalent to E_a having a non-trivial rational point of 4-torsion. This can also be formulated as both the equation of E_a and its 4-division polynomial $f_4(x) = x^6 + ax^2$ having a rational solution. It is easily seen that $P = (a^{1/4}, a^{1/2})$ is always a non-trivial solution to this problem.

Lisoněk [169] used similar techniques to give a different proof of Proposition 7.4.1. Indeed, for $m \geq 3$, $K_m(a)$ is divisible by 8 if and only if E_a has a non-trivial rational point of 8-torsion. This is easily shown to be equivalent to $\mathrm{Tr}_1^m\left(a^{1/4}\right) = \mathrm{Tr}_1^m(a) = 0$.

Finally, it is possible to prove directly that the condition given in Proposition 7.4.2 is not only sufficient, but also necessary, using torsion of elliptic curves[3].

We use this property in Subsection 7.4.2.

Proposition 7.4.4. *Let $a \in \mathbb{F}_{2^m}^*$.*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.*
- *If m is even, then:*
  - *$K_m(a) \equiv 0 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 0$;*
  - *$K_m(a) \equiv -1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 1$.*

Proof. According to Proposition 7.4.2 we only have to show that, if a verifies the given congruence, it can be written as $a = t^4 + t^3$.

- We begin with the case m odd, so that $2^m \equiv -1 \pmod 3$. Then $K_m(a) \equiv 1 \pmod 3$ if and only if $\#E_a \equiv 0 \pmod 3$, i.e. if E_a has a non-trivial rational point of 3-torsion. It implies that the 3-division polynomial of E_a given by $f_3(x) = x^4 + x^3 + a$ has a rational solution, so that there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.
- Suppose now that m is even, so that $2^m \equiv 1 \pmod 3$.
  - If $K_m(a) \equiv -1 \pmod 3$, then $\#E_a \equiv 0 \pmod 3$, and as in the previous case we can find $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.
  - If $K_m(a) \equiv 0 \pmod 3$, then $\#E_a \equiv 1 \pmod 3$, but $\#\widetilde{E}_a \equiv 0 \pmod 3$. The 3-division polynomial of $\widetilde{E}_a$ is also given by $f_3(x) = x^4 + x^3 + a$, so that there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.

□

[3] We were recently made aware that such a result was also proved in a different way also involving elliptic curves by Garashuck and Lisoněk [110] in the case where m is odd

7.4.2 Finding specific values of binary Kloosterman sums

Generic strategy

In this subsection we present the most generic method to find specific values of binary Kloosterman sums. To this end, one picks random elements of $\mathbb{F}_{2^m}$ and computes the corresponding values until a correct one is found. Before performing any complicated computations, divisibility conditions as those stated in the previous section can be used to restrict the pool of elements to those satisfying certain conditions (but without missing any element giving the value searched for) or to filter out elements which will give inadequate values.

Then, the most naive method to check the value of a binary Kloosterman sum is to compute it as a sum. However, one test would need $O(2^m m \log^2 m \log\log m)$ bit operations and this is obviously highly inefficient. Theorem 7.2.1 tells that this costly computation can be replaced by the computation of the cardinality of an elliptic curve over a finite field of even characteristic. Using p-adic methods à la Satoh [229], also known as canonical lift methods, this can be done quite efficiently in $O(m^2 \log^2 m \log\log m)$ bit operations and $O(m^2)$ memory [121, 255, 254, 163]. Working with elliptic curves also has the advantage that one can check that the current curve is a good candidate before computing its cardinality as follows: one picks a random point on the curve and multiplies it by the targeted order; if it does not give the point at infinity, the curve does not have the targeted cardinality.

Finally, it should be noted that, if ones looks for all the elements giving a specific value, a different strategy can be adopted as noted in the paper of Ahmadi and Granger [1]. Recall that a binary Kloosterman sum can be seen as the Walsh–Hadamard transform of the Boolean function $\mathrm{Tr}_1^m(1/x)$. Therefore, we can construct the Boolean function corresponding to the function $\mathrm{Tr}_1^m(1/x)$ and then use a fast Walsh–Hadamard transform to compute the values of all binary Kloosterman sums. Building the Boolean function costs one multiplication per element, so $O(2^m m \log m \log\log m)$ bit operations and $O(2^m)$ memory. The complexity of the fast Walsh–Hadamard transform is $O(2^m m^2)$ bit operations and $O(2^m m)$ memory [2].

Zeros of binary Kloosterman sums

When looking for zeros of binary Kloosterman sums, which is of high cryptographic interest as Chapter 5 [4]emphasizes, one benefits from even more properties of elliptic curves over finite fields. Indeed, when $K_m(a) = 0$, we get that $\#E_a = 2^m$. Hence all rational points of E_a are of order some power of 2.

In fact, we know even more. As E_a is defined over a field of even characteristic, its complete 2^e-torsion (where e is any strictly positive integer) is of rank 1, whereas the complete l^e-torsion, for a prime l different from 2, is of rank 2, as stated in Proposition 7.1.2. Therefore the rational Sylow 2-subgroup is cyclic, isomorphic to $\mathbb{Z}/2^e\mathbb{Z}$ for some positive integer e. In the case where $K_m(a) = 0$, we even get that the whole group of rational points is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$. Furthermore, basic group theory tells that E_a will then have 2^{m-1} points of order 2^m.

Finally, it should be noted that, if $2^m \mid \#E_a$, then $\#E_a$ must be equal to 2^m. This is a simple consequence of Hasse theorem (Theorem 7.1.1) giving bounds on the number of rational points of an elliptic curve over a finite field.

These facts have first been used by Lisoněk [169] to develop a probabilistic method to test whether a given a gives a binary Kloosterman zero or not: one takes a random point on E_a and tests whether its order is 2^m or not. This test involves at most m duplications on the curve, hence is quite efficient. Moreover, as soon as $\#E_a = 2^m$, half of its points are generators, so that

[4]We will see also in Chapter 8 that the value 0 of Kloosterman sums give rise to semi-bent functions in even dimension (see for instance Table 8.1).

testing one point on a correct curve gives a probability of success of 1/2. This led Lisoněk to find zeros of binary Kloosterman sums for m up to 64 in a matter of days.

Afterwards, Ahmadi and Granger [1] proposed a deterministic algorithm to test whether an element $a \in \mathbb{F}_{2^m}$ gives a binary Kloosterman zero or not. From the above discussion, it is indeed enough to compute the size of the Sylow 2-subgroup of E_a to answer that question. This can be efficiently implemented by point halving, starting from a non-trivial point of 4-torsion (remember that such a point always exists on E_a). The complexity of each iteration of their algorithm is dominated by two multiplications in $\mathbb{F}_{2^m}$. So testing a curve with a Sylow 2-subgroup of size 2^e is of complexity $O(e \cdot m \log m \log\log m)$. Furthermore, they showed that the average size of the Sylow 2-subgroup of the curves of the form E_a is 2^3 when m goes to infinity, so that their algorithm has an asymptotic average bit complexity of $O(m \log m \log\log m)$.

Implementation for the value 4

We have seen[5] in Chapter 5 a necessary and sufficient condition to build bent functions from the value 4 of binary Kloosterman sums when m is odd and a necessary only condition when m is even. Unfortunately, the situation is more complicated than in the case of binary Kloosterman zeros.

We are indeed looking for an element $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$. The cardinality of E_a should then be $\#E_a = 2^m + K_m(a) = 4(2^{m-2} + 1)$ which does not ensure to have a completely fixed group structure as was the case when $\#E_a = 2^m$. Moreover, in general, the number $2^{m-2}+1$ does not verify many divisibility properties leading to an efficient test for the value 4. The cardinality of the twist $\widetilde{E}_a$ is given by $\#\widetilde{E}_a = 2^m + 2 - K_m(a) = 2(2^{m-1} - 1)$ which does not provide more useful information.

What we can however deduce from these equalities is that, if $K_m(a) = 4$, then:

- $K_m(a) \equiv 4 \pmod 8$, so that $\mathrm{Tr}_1^m(a) = 1$;
- $K_m(a) \equiv 1 \pmod 3$, so that:
  - if m is odd, then a can be written as $t^4 + t^3$;
  - if m is even, then a can be written as t^3 with $\mathrm{Tr}_2^m(t) \neq 0$.

We can use both these conditions to filter out a to be tested as described in Algorithm 7.1 (for m odd).

We implemented this algorithm in Sage [241]. It was necessary to implement a relatively efficient version of point counting in even characteristic, none of them being available. The first implemented algorithm was an extension to even characteristic of Satoh's original algorithm by Fouquet, Gaudry and Harley [108]. The complexity of this algorithm is $O(m^{3+\epsilon})$ bit operations (or $O(m^5)$ with naive multiplication) and $O(m^3)$ memory, but it is quite simple and there was already an existing implementation in GP/Pari by Yeoh [270] to use as a starting point. The computations in $\mathbb{Z}_{2^m}$, the unique unramified extension of degree m of the 2-adic integers $\mathbb{Z}_2$, were done through the direct library interface to Pari [216] provided in Sage. We also implemented Harley's algorithm [121] as described in Vercauteren's thesis [255] using similar implementation details. . .

.

As a result of our experiments, we found that the following value of a for $m = 55$ gives a value 4 of binary Kloosterman sum. The finite field $\mathbb{F}_{2^{55}}$ is represented as $\mathbb{F}_2[x]/(x^{55} + x^{11} + x^{10} + x^9 +$

[5] We will see also in Chapter 8 that the value 4 of Kloosterman sums give rise to semi-bent functions in even dimension (see for instance Table 8.2).

Algorithm 7.1: Finding the value 4 of binary Kloosterman sums for m odd

Input: A positive odd integer $m \geq 3$
Output: An element $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$

1 $a \leftarrow_R \mathbb{F}_{2^m}$
2 $a \leftarrow a^3(a+1)$
3 **if** $\mathrm{Tr}_1^m(a) = 0$ **then**
4 Go to step 7.1
5 $P \leftarrow_R E_a$
6 **if** $[2^m + 4]P \neq 0$ **then**
7 Go to step 7.1
8 **if** $\#E_a \neq 2^m + 4$ **then**
9 Go to step 7.1
10 **return** a

$x^7 + x^4 + 1$); a is then given as

$$\begin{aligned} a = {} & x^{53} + x^{52} + x^{51} + x^{50} + x^{47} + x^{43} + x^{41} + x^{38} + x^{37} + x^{35} \\ & + x^{33} + x^{32} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} \\ & + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^{12} + x^5 \ . \end{aligned}$$

Chapter 8

Semi-bent functions

Contents

In 1994, the notion of *semi-bent function* has been introduced by Chee, Lee and Kim [62] at Asiacrypt' 94. In fact, these functions had been previously investigated under the name of three-valued almost optimal Boolean functions in [19]. Moreover, they are particular cases of the so-called plateaued functions [276, 275]. Like bent functions, semi-bent functions are also widely studied in cryptography because, besides having low Hadamard transform which provides protection against fast correlation attacks [188] and linear cryptanalysis [182], they can possess desirable properties such as low autocorrelation, propagation criteria, resiliency and high algebraic degree. Semi-bent functions exist for even or odd number of variables. When n is even, the semi-bent functions are those Boolean functions whose Hadamard transform takes values 0 and $\pm 2^{\frac{n+2}{2}}$. They are balanced (up to the addition of a linear function) and have maximal non-linearity among balanced plateaued functions. The maximum-length sequences, also called m-sequences (maximum-length linear feedback shift -register sequences), have received a lot of attention since the late sixties. In terms of linear-feedback shift register (LFSR) synthesis they are usually generated by certain power polynomials over a finite field and in addition are characterized by a low cross correlation and high nonlinearity. Such a sequence is said to be generated by a semi-bent function [59]. Families of maximum-length sequences having three-valued cross-correlation have a wide range of applications in cryptography and code division multiple access (CDMA) communication systems for sequence design [112], [210], [124], [125], [127], [149], [150] etc. However, almost all families of semi-bent functions have been derived from power polynomials $\mathrm{Tr}_1^n\left(x^d\right)$ for a suitably chosen d (see [59] and [242] for the construction of quadratic semi-bent functions in even dimension).

Semi-bent functions exist for even or odd number of inputs.

Definition 8.0.1. *For even n, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$. For odd n, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$.*

It is well known (see for instance [31]) that the algebraic degree of a bent or a semi-bent Boolean function defined on $\mathbb{F}_{2^n}$ is at most $\frac{n}{2}$.

In this manuscript, we will only be interested in even number of inputs where they can be defined as follows.

8.1 Explcit constructions of semi-bent functions in even dimension

In this section, we consider several Boolean functions in univariate representation (expressed by means of the trace function) with even number of variables. Our main intention is to study the relationship between the semi-bentness property of functions obtained with Dillon and Niho exponents . Recall that a *Dillon exponent* is of the form $r(2^m-1)$ where r is co-prime with 2^m+1. Moreover, a positive integer d (always understood modulo 2^n-1) is said to be a *Niho exponent*, and x^d is a *Niho power function*, if the restriction of x^d to $\mathbb{F}_{2^m}$ is linear or in other words $d \equiv 2^j \pmod{2^m-1}$ for some $j < n$) and some exponential sums (namely, Kloosterman sums.

8.1.1 Explcit constructions of semi-bent functions in univariate representation and their links with Kloosterman sums

The goal of this subsection is to investigate the link between the semi-bentness property of some infinite classes of Boolean functions in univariate representation and some exponential sums (Kloosterman sums and cubic sums) ([201], [199]). We shall use the technical results of section 2.3 in Chapter **??**.

We consider infinite families of Boolean functions in univariate representation with even number of variables whose expression is given by (8.1). By computer experiments, for small values of n, we have found that the set of functions of the form (8.1) contains semi-bent functions. We investigate criteria involving Kloosterman sums to determine whether a function of the form (8.1) is semi-bent or not:

$$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) \quad + \mathrm{Tr}_1^n\left(dx^{(2^m-1)s+1}\right) \tag{8.1}$$

where r is a positive integer, $s \in \{0, 1/4, 1/6, 3\}$, $a \in \mathbb{F}_{2^n}^\star$, $b \in \mathbb{F}_4$, $c \in \mathbb{F}_{2^n}$ and $d \in \mathbb{F}_2$. If $b \neq 0$, we consider the functions $g_{a,b,c,d}^{(r,s)}$ of the form (8.1) only when m is odd. Note that $o(r(2^m-1)) = n$, $o(\frac{2^n-1}{3}) = 2$, $o((2^m-1)\frac{1}{2}+1) = m$ and $o((2^m-1)s+1) = n$ for $s \in \{1/4, 1/6, 3\}$ (recall that $o(j)$ denotes the size of the cyclotomic coset of 2 modulo 2^n-1 containing j). Moreover, using the transitivity property of the trace function, we have $\mathrm{Tr}_1^n(cx^{(2^m-1)\frac{1}{2}+1}) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(c^2)x^{2^m+1}) = \mathrm{Tr}_1^m(c'x^{2^m+1})$ where $c' \in \mathbb{F}_{2^m}^\star$. Hence, the polynomial form of $g_{a,b,c,d}^{(r,s)}$ is:

$$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^m(c'x^{2^m+1}) \quad + \mathrm{Tr}_1^n\left(dx^{(2^m-1)s+1}\right)$$

So in the sequel, it suffices to use the previous identity to get the polynomial form of all the presented functions.
Now, we introduce the following decomposition

$$\mathbb{F}_{2^n}^\star = \bigcup_{u\in U} u\mathbb{F}_{2^m}^\star.$$

Let $g_{a,b,c,d}^{(r,s)}$ be any Boolean function of the form (8.1); note that the restriction of $g_{a,b,c,d}^{(r,s)}$ to any coset $u\mathbb{F}_{2^m}^\star$ $(u \in U)$, is affine. More precisely,

- Assume $b \neq 0$. Thanks to the transitivity of the trace function, we have:

$$\forall y \in \mathbb{F}_{2^m}^\star, g_{a,b,c,d}^{(r,s)}(uy) = \mathrm{Tr}_1^m(\alpha_u y) + \beta_u \tag{8.2}$$

with

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_m^n\left(du^{(2^m-1)s+1} + cu^{(2^m-1)\frac{1}{2}+1}\right)\\ &= \mathrm{Tr}_m^n\left(du^{(2^m-1)s+1} + c\right),\\ \beta_u &= \mathrm{Tr}_1^n\left(au^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bu^{\frac{2^n-1}{3}}\right).\end{aligned}$$

- Otherwise (that is, if $b = 0$), thanks to the transitivity of the trace function, we have

$$\forall y \in \mathbb{F}_{2^m}^\star, g_{a,0,c,d}^{(r,s)}(uy) = \mathrm{Tr}_1^m(\alpha_u y) + \beta_u \tag{8.3}$$

with

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_m^n\left(du^{(2^m-1)s+1} + c\right),\\ \beta_u &= \mathrm{Tr}_1^n\left(au^{r(2^m-1)}\right).\end{aligned}$$

Therefore, the Walsh transform of a generic element of the form (8.1) can be computed as follows.

Lemma 8.1.1. *([199]) Using the same notation as in (8.2) or (8.3), for every $\omega \in \mathbb{F}_{2^n}$, the Walsh transform of a generic element of the form (8.1) is*

$$\widehat{\chi_{g_{a,b,c,d}^{(r,s)}}}(\omega) = 1 - \sum_{u\in U}\chi(\beta_u) + 2^m\sum_{u\in U}\delta_0(\alpha_u + \mathrm{Tr}_m^n(\omega u))\chi(\beta_u) \tag{8.4}$$

where δ_0 is the indicator of the singleton $\{0\}$, that is,

$$\delta_0(z) = \begin{cases} 1 & \text{if } z = 0\\ 0 & \text{otherwise}\end{cases}$$

Proof. Suppose m odd and $b \neq 0$. Let $\omega \in \mathbb{F}_{2^n}$. The Walsh transform of $g_{a,b,c,d}^{(r,s)}$ is defined as

$$\widehat{\chi_{g_{a,b,c,d}^{(r,s)}}}(\omega) = \sum_{x\in\mathbb{F}_{2^n}}\chi(g_{a,b,c,d}^{(r,s)}(x) + \mathrm{Tr}_1^n(wx)).$$

Any element $x \in \mathbb{F}_{2^n}^\star$ having a unique polar decomposition $x = uy$ with $u \in U$ and $y \in \mathbb{F}_{2^m}^\star$, we have :

$$\begin{aligned}\widehat{\chi_{g_{a,b,c,d}^{(r,s)}}}(\omega) &= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star} \chi(g_{a,b,c,d}^{(r,s)}(uy) + \mathrm{Tr}_1^n(wuy)) \\ &= 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star} \chi\left(\mathrm{Tr}_1^m\left((\alpha_u + \mathrm{Tr}_m^n(wu))y\right) + \beta_u\right) \\ &= 1 - \sum_{u\in U}\chi(\beta_u) + 2^m \sum_{u\in U}\delta_0(\alpha_u + \mathrm{Tr}_m^n(\omega u))\chi(\beta_u)\end{aligned}$$

Likewise, one can establish (8.4) by similar calculations when $b = 0$ (for any positive integer m). □

We are now going to investigate several subfamilies of (8.1). We begin with a preliminary technical statement.

Lemma 8.1.2. *Let $w \in \mathbb{F}_{2^n}^\star$ and $c \in \mathbb{F}_{2^n}^\star \setminus \mathbb{F}_{2^m}$. The number of $u \in U$ such that $\mathrm{Tr}_m^n(wu+c) = 0$ equals 0 or 2.*

Proof. One has

$$\begin{aligned}\mathrm{Tr}_m^n(wu + c) = 0 \quad &\Longleftrightarrow \quad wu + w^{2^m}u^{2^m} + \mathrm{Tr}_m^n(c) = 0 \\ &\Longleftrightarrow \quad u^2 + w^{-1}\,\mathrm{Tr}_m^n(c)u + w^{2^m-1} = 0.\end{aligned}$$

Now recall that the quadratic equation $X^2 + \alpha X + \beta = 0$, $\alpha \neq 0$, admits 0 or 2 solutions. □

The following result is shown in [93].

Lemma 8.1.3. *[93] For every $w \in \mathbb{F}_{2^n}$,*

- *the equation $\mathrm{Tr}_m^n(wu + u^{\frac{1}{2}}) = 1$ admits 0 or 2 solutions in U, if m is odd.*
- *the equation $\mathrm{Tr}_m^n(wu + u^5) = 1$ admits 0 or 2 solutions in U.*
- *the equation $\mathrm{Tr}_m^n(wu^3 + u^2) + 1 = 0$ admits 0 or 2 solutions in U, if m is even.*

Finally, the next result is shown in [160].

Lemma 8.1.4. *[160]. Let $r > 1$ be a positive integer with $\gcd(r, m) = 1$. Then, the equation $\mathrm{Tr}_m^n(wu) + \sum_{i=1}^{2^{r-1}-1}\mathrm{Tr}_m^n(u^{(2^m-1)\frac{i}{2^r}+1}) = 1$ has 0 or 2 solutions in U for every $w \in \mathbb{F}_{2^n}$.*

In the following we characterize by means of Kloosterman sums the semi-bentness property of functions of the form (8.1) obtained via a Dillon monomial function (that is, a function of the form $\mathrm{Tr}_1^n(ax^{r(2^m-1)})$ where $gcd(r, 2^m + 1) = 1$) and Niho functions. We are going to restrict ourselves the study of the semi-bentness property of $g_{a,b,c,d}^{(r,s)}$ to the case where the coefficient a is in $\mathbb{F}_{2^m}^\star$.

Theorem 8.1.5. *([199]) Let r be a positive integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^\star$ and $c \in \mathbb{F}_{2^n}^\star \setminus \mathbb{F}_{2^m}$. Then the function $g_{a,0,c,0}^{(r,0)}$ is semi-bent if and only if $K_m(a) = 0$. Moreover, suppose that $\mathrm{Tr}_m^n(c) = 1$ then, each function $g_{a,0,c,1}^{(r,\frac{1}{4})}$ (with m odd), $g_{a,0,c,1}^{(r,3)}$ and $g_{a,0,c,1}^{(r,\frac{1}{6})}$ (with m even) is semi-bent if and only if $K_m(a) = 0$.*

Proof. • Let us study the semi-bentness property of the function $g^{(r,0)}_{a,0,c,0}$. Using the notation of (8.3), one has

$$\alpha_u = \mathrm{Tr}_m^n(c), \quad \beta_u = \mathrm{Tr}_1^n(au^{r(2^m-1)}).$$

According to Lemma 8.1.1,

$$\begin{aligned}\widehat{\chi_{g^{(r,0)}_{a,0,c,0}}}(\omega) &= 1 - \sum_{u\in U}\chi(\beta_u) + 2^m \sum_{u\in U}\delta_0(\alpha_u + \mathrm{Tr}_m^n(\omega u))\chi(\beta_u)\\ &= 1 - \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) + 2^m \sum_{u\in U}\delta_0(\mathrm{Tr}_m^n(\omega u + c))\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))\end{aligned}$$

By Lemma 8.1.2, the equation $\mathrm{Tr}_m^n(wu+c) = 0$ admits 0 or 2 solutions in U for every $w \in \mathbb{F}_{2^n}^\star$. Therefore
$\sum_{u\in U}\delta_0(\mathrm{Tr}_m^n(\omega u + c))\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) \in \{0, \pm 2\}$ for every $w \in \mathbb{F}_{2^n}^\star$. In the case where $w = 0$, since $\mathrm{Tr}_m^n(c) \neq 0$ (because $c \in \mathbb{F}_{2^n}^\star \backslash \mathbb{F}_{2^m}$), $\delta_0(\mathrm{Tr}_m^n(c)) = 0$ one gets, $\sum_{u\in U}\delta_0(\mathrm{Tr}_m^n(c))\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) = 0$. Basically, for every $w \in \mathbb{F}_{2^n}$, $\widehat{\chi_{g^{(r,0)}_{a,0,c,0}}}(w) \equiv 1 - \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))\pmod{2^{m+1}}$. Recall that the function $g^{(r,0)}_{a,0,c,0}$ is semi-bent if and only if $\widehat{\chi_{g^{(r,0)}_{a,0,c,0}}}(w) \in \{0, \pm 2^{m+1}\}$ for every $w \in \mathbb{F}_{2^n}$. Now, since

$$-2^{m+1} < -2^m \leq 1 - \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))$$

and

$$1 - \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) \leq 2^m + 2 < 2^{m+1}$$

then, $g^{(r,0)}_{a,0,c,0}$ is semi-bent if and only

$$\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) = 1.$$

Now, since $\gcd(2^m - 1, 2^m + 1) = 1$, the mapping $u \mapsto u^{2^m-1}$ is a permutation of U. The latter condition became

$$\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^r)) = 1.$$

We then conclude thanks to Proposition 2.3.1.

• Let us study the semi-bentness property of the function $g^{(r,\frac{1}{4})}_{a,0,c,1}$. Using the notation of (8.3), one has

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_n^m(c) + \mathrm{Tr}_m^n(u^{(2^m-1)\frac{1}{4}+1}) = 1 + \mathrm{Tr}_m^n(u^{\frac{1}{2}});\\ \beta_u &= \mathrm{Tr}_1^n(au^{r(2^m-1)}).\end{aligned}$$

According to Lemma 8.1.1, the Walsh transform of $g^{(r,\frac{1}{4})}_{a,0,c,1}$ is given by

$$\widehat{\chi_{g^{(r,\frac{1}{4})}_{a,0,c,1}}}(\omega) = 1 - \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) + 2^m \sum_{u\in U}\delta_0(1 + \mathrm{Tr}_m^n(u^{\frac{1}{2}} + \omega u))\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))$$

Thanks to Lemma 8.1.3 (since m is odd), the equation $\mathrm{Tr}_m^n(u^{\frac{1}{2}} + \omega u) = 1$ has 0 or 2 solutions in U for every $w \in \mathbb{F}_{2^n}$. Therefore

$\sum_{u\in U}\delta_0(1+\mathrm{Tr}_m^n(u^{\frac{1}{2}}+\omega u))\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))\in\{0,\pm 2\}$ for every $w\in\mathbb{F}_{2^n}$. Basically, for every $w\in\mathbb{F}_{2^n}$, $\widehat{\chi_{g_{a,0,c,1}^{(r,\frac{1}{4})}}}(w)\equiv 1-\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))\pmod{2^{m+1}}$. Same arguments used as previously lead to $g_{a,0,c,1}^{(r,\frac{1}{4})}$ being semi-bent if and only if $\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))=1$. Using the fact that $u\mapsto u^{2^m-1}$ is a permutation of U, we conclude by Proposition 2.3.1.

• Let us study the semi-bentness property of the function $g_{a,0,c,1}^{(r,3)}$. Using the notation of (8.3), one has

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_n^m(u^{(2^m-1)3+1}+cu^{(2^m-1)\frac{1}{2}+1});\\ \beta_u &= \mathrm{Tr}_1^n(au^{r(2^m-1)}).\end{aligned}$$

Note that $\mathrm{Tr}_n^m(u^{(2^m-1)3+1})=\mathrm{Tr}_n^m(u^{-5})$ and $\mathrm{Tr}_n^m(cu^{(2^m-1)\frac{1}{2}+1})=\mathrm{Tr}_n^m(c)=1$. Hence, $\alpha_u=\mathrm{Tr}_n^m(u^{-5})+1$. According to Lemma 8.1.1, the Walsh transform of $g_{a,0,c,1}^{(r,3)}$ is given by

$$\widehat{\chi_{g_{a,0,c,1}^{(r,3)}}}(\omega)=1-\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))+2^m\sum_{u\in U}\delta_0(\mathrm{Tr}_n^m(u^{-5}+\omega u)+1)\times$$
$$\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))$$

Thanks to Lemma 8.1.3 , the $\mathrm{Tr}_n^m(u^{-5}+\omega u)=1$ admits 0 or 2 solutions in U for every $w\in\mathbb{F}_{2^n}$. Same arguments used as previously lead to $g_{a,0,c,1}^{(r,3)}$ being semi-bent if and only if $\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))=1$. Using the fact that $u\mapsto u^{2^m-1}$ is a permutation of U, we conclude by Proposition 2.3.1.

• Let us study the semi-bentness property of the function $g_{a,0,c,1}^{(r,\frac{1}{6})}$. Using the notation of (8.3), one has

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_n^m(cu^{(2^m-1)\frac{1}{2}+1})+\mathrm{Tr}_m^n(u^{(2^m-1)\frac{1}{6}+1})\\ &= 1+\mathrm{Tr}_m^n(u^{(2^m-1)\frac{1}{6}+1});\\ \beta_u &= \mathrm{Tr}_1^n(au^{r(2^m-1)}).\end{aligned}$$

Note that $u^{(2^m-1)\frac{1}{6}+1}=u^{\frac{2}{3}}$

According to Lemma 8.1.1, the Walsh transform of $g_{a,0,c,1}^{(r,\frac{1}{6})}$ is given by

$$\widehat{\chi_{g_{a,0,c,1}^{(r,\frac{1}{6})}}}(\omega)=1-\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))+2^m\sum_{u\in U}\delta_0(1+\mathrm{Tr}_m^n(u^{\frac{2}{3}}+\omega u))\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})).$$

Thanks to Lemma 8.1.3 (since m is even), the equation $\mathrm{Tr}_m^n(u^2+\omega u^3)+1=0$ admits 0 or 2 solutions in U for every $w\in\mathbb{F}_{2^n}$. But the equation $\mathrm{Tr}_m^n(u^{\frac{2}{3}}+\omega u)=1$ has 0 or 2 solutions in U if and only if the equation $\mathrm{Tr}_m^n(u^2+\omega u^3)+1=0$ admits 0 or 2 solutions in U, for every $w\in\mathbb{F}_{2^n}$. Same arguments used as previously lead to $g_{a,0,c,1}^{(r,\frac{1}{6})}$ being semi-bent if and only if $\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))=1$. We conclude by Proposition 2.3.1.

□

Remark 8.1.6. *The function $g_{a,0,c,0}^{(r,0)}$ has algebraic degree m, maximal possibly for a semi-bent. Indeed, the exponent $r(2^m-1)$ is of 2-weight m while the exponent $(2^m-1)1/2+1$ is of 2-weight 2. Moreover, $\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$ and $\mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ are two separate parts in the trace representation of $g_{a,0,c,0}^{(r,0)}$. Likewise, the functions $g_{a,0,c,1}^{(r,\frac{1}{4})}$, $g_{a,0,c,1}^{(r,3)}$ and $g_{a,0,c,1}^{(r,\frac{1}{6})}$ have algebraic degree*

equal to m (the exponents $r(2^m-1)$, $(2^m-1)3+1$ and $(2^m-1)1/6+1$ are of 2-weight m while the exponents $(2^m-1)1/2+1$ and $(2^m-1)1/4+1$ are of respectively algebraic degrees 2 and 3 (as observed in [93]).

Theorem 8.1.7. *([199]) Let $n=2m$ with $m>3$ odd. Let r be a positive integer such that $gcd(r,2^m+1)=1$. Let $a\in\mathbb{F}_{2^m}^\star$, $b\in\mathbb{F}_4^\star$ and $c\in\mathbb{F}_{2^n}^\star\setminus\mathbb{F}_{2^m}$. Then, the function $g_{a,b,c,0}^{(r,0)}$ is semi-bent if and only if $K_m(a)=4$. Moreover, suppose that $\mathrm{Tr}_m^n(c)=1$ then, each function $g_{a,b,c,1}^{(r,\frac{1}{4})}$ and $g_{a,b,c,1}^{(r,3)}$ is semi-bent if and only if $K_m(a)=4$.*

Proof. • Let us study the semi-bentness property of the function $g_{a,b,c,0}^{(r,0)}$. Using the notation of (8.2), one has

$$\alpha_u=\mathrm{Tr}_m^n(c),\quad \beta_u=\mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}).$$

Since α_u is the same as the one associated to $g_{a,0,c,0}^{(r,0)}$ in the proof of Theorem 8.1.5 then, using the same arguments as those exposed in the beginning of the proof of Theorem 8.1.5, we get that $g_{a,b,c,0}^{(r,0)}$ is semi-bent if and only if

$$\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}))=1.$$

We finally conclude thanks to Corollary 2.3.3.

• Let us study the semi-bentness property of the function $g_{a,b,c,1}^{(r,\frac{1}{4})}$. Using the notation of (8.2), one has

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_n^m(c)+\mathrm{Tr}_m^n(u^{(2^m-1)\frac{1}{4}+1});\\ \beta_u &= \mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}).\end{aligned}$$

Note that, $\mathrm{Tr}_m^n(u^{(2^m-1)\frac{1}{4}+1})=\mathrm{Tr}_m^n(u^{\frac{1}{2}})$. Then, (since $\mathrm{Tr}_m^n(c)=1$, by hypothesis) $\alpha_u=1+\mathrm{Tr}_m^n(u^{\frac{1}{2}})$.

According to Lemma 8.1.1, the Walsh transform of $g_{a,b,c,1}^{(r,\frac{1}{4})}$ is given by

$$\begin{aligned}\widehat{\chi_{g_{a,b,c,1}^{(r,\frac{1}{4})}}}(\omega)&=1-\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}))\\ &\quad+2^m\sum_{u\in U}\delta_0(1+\mathrm{Tr}_m^n(u^{\frac{1}{2}}+\omega u))\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}})).\end{aligned}$$

Thanks to Lemma 8.1.3 (since m is odd), the equation $\mathrm{Tr}_m^n(u^{\frac{1}{2}}+\omega u)=1$ has 0 or 2 solutions in U for every $w\in\mathbb{F}_{2^n}$. Same arguments being used in the proof of Theorem 8.1.5 lead to $g_{a,b,c,1}^{(r,\frac{1}{4})}$ semi-bent if and only if $\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}})=1$. Using the fact that $u\mapsto u^{2^m-1}$ is a permutation of U, we conclude thanks to Corollary 2.3.3.

• Let us study the semi-bentness property of the function $g_{a,b,c,1}^{(r,3)}$. Using the notation of (8.2), one has

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_n^m(u^{(2^m-1)3+1})+cu^{(2^m-1)\frac{1}{2}+1});\\ \beta_u &= \mathrm{Tr}_1^n(au^{r(2^m-1)})+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}).\end{aligned}$$

Same arguments used as previously lead to $g^{(r,3)}_{a,b,c,1}$ being semi-bent if and only if

$$\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}})=1.$$

We conclude thanks to Corollary 2.3.3.

□

Remark 8.1.8. *The function $g^{(r,0)}_{a,b,c,0}$ has algebraic degree m, maximal algebraic degree for a semi-bent. Indeed, the two exponents $r(2^m-1)$ and $\frac{2^n-1}{3}$ are of 2-weight m (since $\frac{2^n-1}{3}=1+4+\cdots+4^{m-1}$). Hence, the two Boolean functions $x\mapsto \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$ and $x\mapsto \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ are of algebraic degree equal to m, while the function $x\mapsto \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ is of algebraic degree equals 2. Moreover, $\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$, $\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$ and $\mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ are three separate parts in the trace representation of $g^{(r,0)}_{a,b,c,0}$. Likewise, the functions $g^{(r,\frac{1}{4})}_{a,0,c,1}$ and $g^{(r,3)}_{a,b,c,1}$ have algebraic degree equal to m.*

Example 8.1.9. *Let us describe for instance, the set of semi-bent Boolean functions $g^{(1,0)}_{a,b,c,0}$ defined on $\mathbb{F}_{2^{10}}$ of the form $\mathrm{Tr}_1^{10}(ax^{31})+\mathrm{Tr}_1^2(bx^{341})+\mathrm{Tr}_1^{10}(cx^{528})$ where $a\in\mathbb{F}_{2^5}^\star$, $b\in\mathbb{F}_4^\star$, $c\in\mathbb{F}_{2^{10}}^\star\setminus\mathbb{F}_{2^5}$. Let β be a primitive element of $\mathbb{F}_4$ and α be a primitive element of $\mathbb{F}_{32}=\mathbb{F}_2(\alpha)$ with $\alpha^5+\alpha^2+1=0$. Recall that according to Proposition 2, $K_5(a)\equiv 1 \pmod 3$ if and only if $\mathrm{Tr}_1^5(a^{1/3})=0$. Now, according to table 4 in [56], $E_0:=\{a\in\mathbb{F}_{2^5}^\star,\mathrm{Tr}_1^5(a^{1/3})=0\}=\{\alpha^3,\alpha^{21},\alpha^{14}\}$, $\{a\in\mathbb{F}_{2^5}^\star,K_5(a)=4\}=\{\alpha^3,\alpha^{21}\}$ and $E_1:=\{a\in\mathbb{F}_{2^5}^\star,\mathrm{Tr}_1^5(a^{1/3})=1\}=\{1,\alpha^2,\alpha^9,\alpha^{15}\}$. Then, according to Theorem 8.1.7, the functions $g^{(1,0)}_{\alpha^3,1,c,0}$, $g^{(1,0)}_{\alpha^3,\beta,c,0}$, $g^{(1,0)}_{\alpha^3,\beta^2,c,0}$, $g^{(1,0)}_{\alpha^{21},1,c,0}$, $g^{(1,0)}_{\alpha^{21},\beta,c,0}$, $g^{(1,0)}_{\alpha^{21},\beta^2,c,0}$ are semi-bent while $g^{(1,0)}_{\alpha^{14},1,c,0}$, $g^{(1,0)}_{\alpha^{14},\beta,c,0}$, $g^{(1,0)}_{\alpha^{14},\beta^2,c,0}$, $g^{(1,0)}_{a,1,c,0}$, $g^{(1,0)}_{a,\beta,c,0}$,$g^{(1,0)}_{a,\beta^2,c,0}$ are not semi-bent if $a\in\{1,\alpha^2,\alpha^9,\alpha^{15}\}$.*

Now, we are interested in studying the semi-bentness property of functions of the form $g^{(3,0)}_{a,b,c,0}$ with m odd, $a\in\mathbb{F}_{2^n}^\star$, $b\in\mathbb{F}_4^\star$ and $c\in\mathbb{F}_{2^n}^\star$ (note that the function $x\mapsto\mathrm{Tr}_1^n(ax^{3(2^m-1)})$ is not a Dillon monomial function since 3 is not co-prime with 2^m+1 when m is odd). To this end, we show that we can identify all the semi-bent functions in the form $g^{(3,0)}_{a,b,c,0}$ by studying only the semi-bentness of $g^{(3,0)}_{a\zeta^i,b,c,0}$ where $a\in\mathbb{F}_{2^m}^\star$, $b\in\mathbb{F}_4^\star$, $c\in\mathbb{F}_{2^n}^\star$, ζ is a generator of the cyclic group U and $i\in\{0,1\}$. Let $a\in\mathbb{F}_{2^m}^\star$, $\lambda\in\mathbb{F}_{2^n}^\star$, $b\in\mathbb{F}_4^\star$ and $c\in\mathbb{F}_{2^n}^\star$. Set $a'=a\lambda^{3(2^m-1)}$, $b'=b\lambda^{\frac{2^n-1}{3}}$ and $c'=c\lambda^{(2^m-1)\frac{1}{2}+1}$. Then remark that, for every $x\in\mathbb{F}_{2^n}$, we have:

$$\begin{aligned}g^{(3,0)}_{a',b',c',0}(x)&=\mathrm{Tr}_1^n(a(\lambda x)^{3(2^m-1)})+\mathrm{Tr}_1^2(b(\lambda x)^{\frac{2^n-1}{3}})\\&\quad+\mathrm{Tr}_1^n(c\lambda^{(2^m-1)\frac{1}{2}+1}x^{(2^m-1)\frac{1}{2}+1})\\&=g^{(3,0)}_{a,b,c,0}(\lambda x)\end{aligned}$$

This means that $g^{(3,0)}_{a',b',c',0}$ is linearly equivalent to $g^{(3,0)}_{a,b,c,0}$. Therefore, we don't have to consider all the possible values of $a\in\mathbb{F}_{2^n}^\star$ in our study. Indeed, recall that every element of x in $\mathbb{F}_{2^n}^\star$ admits a unique polar decomposition $x=uy$ with $y\in\mathbb{F}_{2^m}^\star$ and $u\in U$. Now, m being odd, every element $u\in U$ can be uniquely decomposed as $u=\zeta^i v$ with $i\in\{0,1,2\}$ and $v\in V=\{u^3\mid u\in U\}$. One deduces

Lemma 8.1.10. *([199]) Let $n=2m$ with m odd. Let $a'\in\mathbb{F}_{2^n}^\star$, $b'\in\mathbb{F}_4^\star$, $c'\in\mathbb{F}_{2^n}^\star$. Suppose that $a'=a\zeta^i v$ with $a\in\mathbb{F}_{2^m}^\star$ $i\in\{0,1,2\}$, ζ a generator of the cyclic group U and, $v\in V=\{u^3\mid u\in U\}$. Then, there exist $b\in\mathbb{F}_4^\star$ and $c\in\mathbb{F}_{2^n}^\star$ such that $g^{(3,0)}_{a',b',c',0}$ is linearly equivalent to $g^{(3,0)}_{a\zeta^i,b,c,0}$.*

Every element $a' \in \mathbb{F}_{2^n}^\star$ can be (uniquely) decomposed as $a' = a\zeta^i v$ with a, ζ and v as in the preceding lemma. The property of semi-bentness being affine invariant, one can restrict oneself to study the semi-bentness of $g^{(3,0)}_{a\zeta^i,b,c,0}$ with $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4^\star$, $c \in \mathbb{F}_{2^n}^\star$ and $i \in \{0,1\}$.

Theorem 8.1.11. *([199]) Let $n = 2m$ with m odd, $a \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4^\star$, $c \in \mathbb{F}_{2^n}^\star \setminus \mathbb{F}_{2^m}$ and ζ be a generator of U.*

1. *Assume $m \equiv 3 \pmod 6$. Then the functions $g^{(3,0)}_{a,b,c,0}$ and $g^{(3,0)}_{a\zeta,b,c,0}$ are not semi-bent.*
2. *Assume $m \not\equiv 3 \pmod 6$. Then, $g^{(3,0)}_{a\zeta^i,b,c,0}$ is semi-bent if and only if*
   - *$i = 0$ and $K_m(a) = 4$,*
   - *or, $i = 1$ and $K_m(a) + C_m(a,a) = 4$.*

Proof. Let $i \in \{0,1\}$. Using the notation of (8.2), one has

$$\beta_u = \mathrm{Tr}_1^n(a\zeta^i u^{3(2^m-1)}) + \mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}), \quad \alpha_u = \mathrm{Tr}_m^n(c).$$

Same arguments as in the beginning of the proof of Theorem 8.1.5 lead to $g^{(3,0)}_{a\zeta^i,b,c,0}$ being semi-bent if and only if

$$\sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(a\zeta^i u^{3(2^m-1)}) + \mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}})\right) = 1$$

equivalently (since the mapping $u \mapsto u^{2^m-1}$ is a permutation on U)

$$\sum_{u\in U} \chi\left(\mathrm{Tr}_1^n(a\zeta^i u^3) + \mathrm{Tr}_1^2(bu^{\frac{2^m+1}{3}})\right) = 1.$$

Assertions (1) and (2) then follow from Corollary 2.3.5. □

Remark 8.1.12. *The function $g^{(3,0)}_{a\zeta^i,b,c,0}$ has algebraic degree m, maximal algebraic degree for a semi-bent. Indeed, the exponents $3(2^m-1)$ and $(2^n-1)/3$ are of 2-weight m (since $3(2^m-1) = 1 + 2^2 + 2^3 + \cdots + 2^{m-1} + 2^{m+1}$) while the exponent $(2^m-1)\frac{1}{2}+1$ is of 2-weight 2. Moreover, $\mathrm{Tr}_1^n\left(a\zeta^i x^{3(2^m-1)}\right)$, $\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$ and $\mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ are three separate parts in the trace representation of $g^{(3,0)}_{a\zeta^i,b,c,0}$.*

In the following we characterize by means of Kloosterman sums the semi-bentness property of functions obtained via a Dillon monomial function and 2^r Niho power functions.

Theorem 8.1.13. *([199]) Let $n = 2m$, r be a positive integer such that $gcd(r, 2^m+1) = 1$, $\nu > 1$ be a positive integer with $\gcd(\nu, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_m^n(\alpha) = 1$, $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_4^\star$.*

Let f be the Boolean function defined over $\mathbb{F}_{2^n}$ whose expression is given by

$$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(\alpha x^{2^m+1} + \sum_{i=1}^{2^{\nu-1}-1} x^{(2^m-1)\frac{i}{2^\nu}+1}\right)$$

Let g be the Boolean function defined over $\mathbb{F}_{2^n}$ (m odd) whose expression is given by $g(x) = f(x) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$. Then, the function f (Resp. g) is semi-bent if and only if, $K_m(a) = 0$ (Resp. $K_m(a) = 4$).

Proof. • Let us study the semi-bentness property of the function f. Using the notation of (8.3), one has

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_n^m(\alpha^{\frac{1}{2}} + \sum_{i=1}^{2^{\nu-1}-1} u^{(2^m-1)\frac{i}{2^\nu}+1});\\ \beta_u &= \mathrm{Tr}_1^n(au^{r(2^m-1)}).\end{aligned}$$

According to Lemma 8.1.1, the Walsh transform of f is given by

$$\begin{aligned}\widehat{\chi_f}(\omega) = 1 &- \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))\\ &+ 2^m\sum_{u\in U}\delta_0(\mathrm{Tr}_n^m(\alpha^{\frac{1}{2}} + \sum_{i=1}^{2^{\nu-1}-1} u^{(2^m-1)\frac{i}{2^\nu}+1}) + \omega u))\times\\ &\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})).\end{aligned}$$

Thanks to Lemma 8.1.4, the equation $\mathrm{Tr}_m^n(wu)+\sum_{i=1}^{2^{\mu-1}-1}\mathrm{Tr}_m^n(u^{(2^m-1)\frac{i}{2^\mu}+1}) = 1$ admits 0 or 2 solutions in U for every $w\in\mathbb{F}_{2^n}$. Since $\mathrm{Tr}_m^n(\alpha) = 1$ (by hypothesis) and $\mathrm{Tr}_m^n((\alpha^{\frac{1}{2}})^2) = \mathrm{Tr}_m^n(\alpha^{\frac{1}{2}})$, the equation $\mathrm{Tr}_n^m(\sum_{i=1}^{2^{\nu-1}-1} u^{(2^m-1)\frac{i}{2^\nu}+1}) + \omega u) = 1$ admits 0 or 2 solutions in U for every $w\in\mathbb{F}_{2^n}$. Same arguments used in the proof of Theorem 8.1.5 lead to f being semi-bent if and only $\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) = 1$. We conclude by Proposition 2.3.1.
• Let study us the semi-bentness property of the function g. Using the notation of (8.2), one has

$$\begin{aligned}\alpha_u &= \mathrm{Tr}_n^m(\alpha^{\frac{1}{2}} + \sum_{i=1}^{2^{\nu-1}-1} u^{(2^m-1)\frac{i}{2^\nu}+1});\\ \beta_u &= \mathrm{Tr}_1^n(au^{r(2^m-1)}) + \mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}).\end{aligned}$$

Same arguments used as previously lead to g being semi-bent if and only $\sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))+\mathrm{Tr}_1^2(bu^{\frac{2^n-1}{3}}) = 1$. We conclude thanks to Corollary 2.3.3. □

8.1.2 Semi-bent functions in polynomial forms with multiple trace terms and their link with Dikson polynomial

In this subsection, we study the relationship between the semi-bentness property of functions in polynomial forms with multiple trace terms and Dickson polynomials.

In the following, we are interested in semi-bent functions whose expression contains multiple trace terms. Let E be a set of representatives of the cyclotomic classes modulo 2^n-1 for which each class has full size n. Let $f_{a_r,b,c}$ be the function defined on $\mathbb{F}_{2^n}$ whose polynomial form is given by

$$\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}) + \mathrm{Tr}_1^m(cx^{2^m+1}) \tag{8.5}$$

where $R\subseteq E$, $a_r\in\mathbb{F}_{2^m}^\star$, $b\in\mathbb{F}_4^\star$ and $c\in\mathbb{F}_{2^m}^\star$. In the following, we will show that semi-bent functions $f_{a_r,b,c}$ of the form (8.5) can be described by means of exponential sums involving the Dickson polynomials. In particular, one can provide a way to transfer the characterization of semi-bentness of a function of the form (8.5) to the evaluation of the Hamming weight of some Boolean functions.

To prove the result of this subsection, we need the following statements (Proposition 8.1.14) and Corollary 8.1.15).

Proposition 8.1.14. *([199]) For $b \in \mathbb{F}_4^\star$ and $a_r \in \mathbb{F}_{2^m}^\star$, we denote by $g_{a_r,b}$ the function $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ and by $g_{a_r,0}$ the function $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$. Let V be the set of the elements of the cubes of U and ζ be a generator of U. Then, we have the following relations:*

$$\sum_{u\in U} \chi\Big(g_{a_r,\beta}(u)\Big) = \sum_{u\in U} \chi\Big(g_{a_r,\beta^2}(u)\Big) = -\sum_{v\in V} \chi\Big(g_{a_r,0}(v)\Big) \tag{8.6}$$

and

$$\sum_{u\in U} \chi\Big(g_{a_r,1}(u)\Big) = \sum_{v\in V} \chi\Big(g_{a_r,0}(v)\Big) - 2\sum_{v\in V} \chi\Big(g_{a_r,0}(\zeta v)\Big) \tag{8.7}$$

Proof. Introduce for every element b' of $\mathbb{F}_4$, the sum

$$\Lambda(b') := \sum_{b\in\mathbb{F}_4}\sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big)\chi\Big(\mathrm{Tr}_1^2(bb')\Big).$$

Note that

$$\Lambda(b') = \sum_{u\in U} \chi\Big(g_{a_r,0}(u)\Big) \sum_{b\in\mathbb{F}_4} \chi\Big(\mathrm{Tr}_1^2\Big(b\big(b' + u^{\frac{2^n-1}{3}}\big)\Big)\Big).$$

Furthermore, one has

$$\sum_{b\in\mathbb{F}_4} \chi\Big(\mathrm{Tr}_1^2\Big(b\Big(b' + u^{\frac{2^n-1}{3}}\Big)\Big)\Big) = \begin{cases} 0 \text{ if } u^{\frac{2^n-1}{3}} \neq b' \\ 4 \text{ otherwise} \end{cases}$$

Since, $u^{\frac{2^n-1}{3}} \neq 0$ for every $u \in U$, $\Lambda(0) = 0$. Since β is a primitive element of $\mathbb{F}_4$, suppose that $b' = \beta^i$ for $i \in \{0,1,2\}$. Then, for a generator ζ of U, we have, $\beta^i = \zeta^{i\frac{2^m+1}{3}}$. Hence,

$$\begin{aligned}\Lambda(\beta^i) &= 4 \sum_{u\in U,\, u^{\frac{2^n-1}{3}} = \zeta^{i\frac{2^m+1}{3}}} \chi\Big(g_{a_r,0}(u)\Big) \\ &= 4 \sum_{u\in U,\, (u^{-2}\zeta^{-i})^{\frac{2^m+1}{3}} = 1} \chi\Big(g_{a_r,0}(u)\Big) \\ &= 4 \sum_{u\in U,\, u^{-2}\in\zeta^i V} \chi\Big(g_{a_r,0}(u)\Big).\end{aligned}$$

That follows from the fact that the only elements x of U such that $x^{\frac{2^m+1}{3}} = 1$ are the elements of V. Next, note that the map $x \mapsto x^{2^{m-1}}$ is one-to-one from $\zeta^i V$ to $\zeta^i V$ (since $\zeta^{i(2^{m-1}-1)}$ is a cube because $2^{m-1} - 1 \equiv 0 \pmod 3$ for m odd), one gets that $u^{\frac{2^n-1}{3}} = \zeta^{i\frac{2^m+1}{3}}$ if and only if $u \in \zeta^i V$.

Therefore,

$$\Lambda(\beta^i) = 4\sum_{v\in V} \chi\Big(g_{a_r,0}(\zeta^i v)\Big). \tag{8.8}$$

Now, establish an expression of $\sum_{b'\in\mathbb{F}_4}\Lambda(b')\chi\Big(\mathrm{Tr}_1^2(bb')\Big)$ involving $\sum_{u\in U}\chi\Big(g_{a_r,b}(u)\Big)$.

$$\begin{aligned}
&\sum_{b'\in\mathbb{F}_4}\Lambda(b')\chi\Big(\mathrm{Tr}_1^2(bb')\Big)\\
&=\sum_{b'\in\mathbb{F}_4}\sum_{b''\in\mathbb{F}_4}\sum_{u\in U}\chi\Big(g_{a_r,b''}(u)\Big)\chi\Big(\mathrm{Tr}_1^2(b''b')\Big)\chi\Big(\mathrm{Tr}_1^2(bb')\Big)\\
&=\sum_{b''\in\mathbb{F}_4}\sum_{u\in U}\chi\Big(g_{a_r,b''}(u)\Big)\sum_{b'\in\mathbb{F}_4}\chi\Big(\mathrm{Tr}_1^2(b'(b''+b))\Big).
\end{aligned}$$

Since,

$$\sum_{b'\in\mathbb{F}_4}\chi\Big(\mathrm{Tr}_1^2(b'(b''+b))\Big)=\begin{cases}4 \text{ if } b''=b\\ 0 \text{ otherwise}\end{cases}$$

then, one gets

$$\sum_{b'\in\mathbb{F}_4}\Lambda(b')\chi\Big(\mathrm{Tr}_1^2(bb')\Big)=4\sum_{u\in U}\chi\Big(g_{a_r,b}(u)\Big)$$

that is,

$$\sum_{u\in U}\chi\Big(g_{a_r,b}(u)\Big)=\frac{1}{4}\sum_{b'\in\mathbb{F}_4}\Lambda(b')\chi\Big(\mathrm{Tr}_1^2(bb')\Big). \tag{8.9}$$

Finally, by formula (8.8), one gets (since $\chi(\mathrm{Tr}_1^2(1))=1$ and $\chi(\mathrm{Tr}_1^2(\beta))=\chi(\mathrm{Tr}_1^2(\beta^2))=-1$)

$$\begin{aligned}
\sum_{u\in U}\chi\Big(g_{a_r,1}(u)\Big)&=\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big)\\
&\quad-\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta v)\Big)-\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta^2 v)\Big).\\
\sum_{u\in U}\chi\Big(g_{a_r,\beta}(u)\Big)&=-\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big)\\
&\quad-\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta v)\Big)+\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta^2 v)\Big).\\
\sum_{u\in U}\chi\Big(g_{a_r,\beta^2}(u)\Big)&=-\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big)\\
&\quad+\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta v)\Big)-\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta^2 v)\Big).
\end{aligned}$$

To conclude, note that one has

$$\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta v)\Big)=\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta^2 v)\Big) \tag{8.10}$$

Indeed, since the trace function is invariant under the Frobenius automorphism $x\mapsto x^2$, we get, applying m times, the Frobenius automorphism : $\forall x\in\mathbb{F}_{2^n}$,

$$g_{a_r,0}(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r^{2^m}x^{2^m r(2^m-1)}\right)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{2^m r(2^m-1)}\right)=g_{a_r,0}(x^{2^m})$$

because the a_r's are in $\mathbb{F}_{2^m}^\star$. Hence,

$$\begin{aligned}&\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta v)\Big)\\&=\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta^{2^m}v^{2^m})\Big)\\&=\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta^2(\zeta^{2^m-2}v^{2^m}))\Big).\end{aligned}$$

Now, since m is odd, 3 divides 2^m+1 and thus divides 2^m-2. Hence, ζ^{2^m-2} is a cube of U and the mapping $v\mapsto\zeta^{(2^m-2)}v^{2^m}$ is a permutation of V. The relation (8.10) follows. □

Corollary 8.1.15. *([199]) For $b\in\mathbb{F}_4^\star$ and $a_r\in\mathbb{F}_{2^m}^\star$, we denote by $g_{a_r,b}$ the function defined on $\mathbb{F}_{2^n}$ by $\sum_{r\in R}\mathrm{Tr}_1^n(a_rx^{r(2^m-1)})+\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$, and by h_{a_r} the function defined on $\mathbb{F}_{2^m}$ by $h_{a_r}(x)=\sum_{r\in R}\mathrm{Tr}_1^m(a_rD_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then,*

1. *$\sum_{u\in U}\chi\Big(g_{a_r,\beta}(u)\Big)=1$ if and only if $\sum_{u\in U}\chi\Big(g_{a_r,\beta^2}(u)\Big)=1$ if and only if,*

$$\begin{aligned}&\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_3(x))\Big)\\&\qquad=2^m-2\,\mathrm{wt}(h_{a_r}\circ D_3)+4.\end{aligned}$$

2. *$\sum_{u\in U}\chi\Big(g_{a_r,1}(u)\Big)=1$ if and only if*

$$\begin{aligned}&3\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(x)\Big)\\&-2\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_3(x))\Big)\\&=4+2^m+4\,\mathrm{wt}(h_{a_r}\circ D_3)-6\,\mathrm{wt}(h_{a_r}).\end{aligned}$$

To prove the corollary, we need the following useful lemma.

Lemma 8.1.16. *([199]) Keeping the same notations as in Corollary 8.1.15, for any positive integer p, we have*

$$\sum_{u\in U}\chi\Big(g_{a_r,0}(u^p)\Big)=1+\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_p(x))\Big)-\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_p(x))\Big).$$

Proof. Thanks to Lemma **??**, one gets

$$\sum_{u\in U}\chi\Big(g_{a_r,0}(u^p)\Big)=1+2\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(h_{a_r}(D_p(x))\Big).$$

Now, note that the indicator of the set $\{x\in\mathbb{F}_{2^m}^\star\mid\mathrm{Tr}_1^m(x^{-1})=1\}$ can be written as

$\frac{1}{2}\left(1-\chi(\mathrm{Tr}_1^m(x^{-1}))\right)$. Hence, $\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(h_{a_r}(D_p(x))\Big)$

$$\begin{aligned}
&= \frac{1}{2}\sum_{x\in\mathbb{F}_{2^m}^\star}\chi\Big(h_{a_r}(D_p(x))\Big)\\
&- \frac{1}{2}\sum_{x\in\mathbb{F}_{2^m}^\star}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_p(x))\Big)\\
&= \frac{1}{2}\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_p(x))\Big)\\
&- \frac{1}{2}\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_p(x))\Big).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\sum_{u\in U}\chi\Big(g_{a_r,0}(u^p)\Big) &= 1+\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_p(x))\Big)\\
&- \sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_p(x))\Big).
\end{aligned}$$

□

Now, we prove Corollary 8.1.15.

Proof. 1. According to Proposition 8.1.14, $\sum_{u\in U}\chi\Big(g_{a_r,\beta}(u)\Big)=1$ if and only if,

$$\sum_{u\in U}\chi\Big(g_{a_r,\beta^2}(u)\Big)=1$$

if and only if,

$$\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big)=-1.$$

We have

$$\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big)=\frac{1}{3}\sum_{u\in U}\chi\Big(g_{a_r,0}(u^3)\Big)$$

Now, take $p=3$ in Lemma 8.1.16:

$$\sum_{u\in U}\chi\Big(g_{a_r,0}(u^3)\Big)=1+\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_3(x))\Big)-\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_3(x))\Big).$$

Hence $\sum_{u\in U}\chi\Big(g_{a_r,\beta}(u)\Big)=1$ if and only if, $\sum_{u\in U}\chi\Big(g_{a_r,\beta^2}(u)\Big)=1$) if and only if,

$$\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_3(x))\Big)=4+\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_3(x))\Big).$$

Now, using the fact that, for a Boolean function f defined on $\mathbb{F}_{2^n}$, $\sum_{x\in\mathbb{F}_{2^n}}\chi\Big(f(x)\Big)=2^n-2\,\mathrm{wt}(f)$, we finally get that $\sum_{u\in U}\chi\Big(g_{a_r,\beta}(u)\Big)=1$ if and only if, $\sum_{u\in U}\chi\Big(g_{a_r,\beta^2}(u)\Big)=1$ if and only if,

$$\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_3(x))\Big)=4+2^m-2\,\mathrm{wt}(h_{a_r}\circ D_3).$$

The assertion 1) follows.

2. By Proposition 8.1.14, $\sum_{u\in U}\chi\Big(g_{a_r,1}(u)\Big)=1$ if and only if,

$$\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big)-2\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta v)\Big)=1.$$

Note that we have

$$\sum_{u\in U}\chi\Big(g_{a_r,0}(u)\Big)=\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big)+\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta v)\Big)+\sum_{v\in V}\chi\Big(g_{a_r,0}(\zeta^2 v)\Big)$$

Using relation (8.10) and the fact that $\sum_{v\in V}\chi(g_{a_r,0}(v))=\frac{1}{3}\sum_{u\in U}\chi(g_{a_r,0}(u^3))$, one gets $\sum_{u\in U}\chi\Big(g_{a_r,1}(u)\Big)=1$ if and only if, $\frac{2}{3}\sum_{u\in U}\chi(g_{a_r,0}(u^3))-\sum_{u\in U}\chi(g_{a_r,0}(u))=1$.
Now, apply Lemma 8.1.16 for $p=3$ and $p=1$:

$$\sum_{u\in U}\chi\Big(g_{a_r,0}(u^3)\Big)=1+\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_3(x))\Big)-\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_3(x))\Big)$$

and (since $D_1(x)=x$)

$$\sum_{u\in U}\chi\Big(g_{a_r,0}(u)\Big)=1+\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(x)\Big)-\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(x)\Big).$$

The condition

$$\frac{2}{3}\sum_{u\in U}\chi(g_{a_r,0}(u^3))-\sum_{u\in U}\chi(g_{a_r,0}(u))=1$$

is then equivalent to

$$\begin{aligned}&2/3+2/3\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_3(x))\Big)-2/3\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(D_3(x))\Big)\\&-1-\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(x)\Big)+\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(\mathrm{Tr}_1^m(x^{-1})+h_{a_r}(x)\Big)=1.\end{aligned}$$

Now,

$$\sum_{x\in\mathbb{F}_{2^m}}\chi\Big(h_{a_r}(D_3(x))\Big)=2^m-2\,\mathrm{wt}(h_{a_r}\circ D_3)$$

and

$$\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(h_{a_r}(x)\Big) = 2^m - 2\,\mathrm{wt}(h_{a_r}).$$

The latter condition is equivalent to

$$\begin{aligned} &2/3 + 2/3(2^m - 2\,\mathrm{wt}(h_{a_r}\circ D_3)) - 2/3\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + h_{a_r}(D_3(x))\Big)\\ &-1 - (2^m - 2\,\mathrm{wt}(h_{a_r})) + \sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + h_{a_r}(x)\Big) = 1. \end{aligned}$$

that is,

$$\begin{aligned} &3\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + h_{a_r}(x)\Big) - 2\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + h_{a_r}(D_3(x))\Big)\\ &= 4 + 2^m + 4\,\mathrm{wt}(h_{a_r}\circ D_3) - 6\,\mathrm{wt}(h_{a_r}). \end{aligned}$$

□

Using the previous results, we prove the following characterization of semi-bentness for functions in the form (8.5).

Theorem 8.1.17. *([199]) Let $n = 2m$ with m odd. Let $b \in \mathbb{F}_4^\star$, β be a primitive element of $\mathbb{F}_4$ and $c \in \mathbb{F}_{2^m}^\star$. Let $f_{a_r,b,c}$ be the function defined on $\mathbb{F}_{2^n}$ whose expression is of the form (8.5). Let h_{a_r} be the related function defined on $\mathbb{F}_{2^m}$ by $h_{a_r}(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then*

1. *$f_{a_r,\beta,c}$ is semi-bent if and only if, $f_{a_r,\beta^2,c}$ is semi-bent, if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + h_{a_r}(D_3(x))\Big) = 2^m - 2\,\mathrm{wt}(h_{a_r}\circ D_3) + 4.$$

2. *$f_{a_r,1,c}$ is semi-bent if and only if,*

$$\begin{aligned} &3\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + h_{a_r}(x)\Big) - 2\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + h_{a_r}(D_3(x))\Big)\\ &= 4 + 2^m + 4\,\mathrm{wt}(h_{a_r}\circ D_3) - 6\,\mathrm{wt}(h_{a_r}). \end{aligned}$$

Proof. For $b \in \mathbb{F}_4^\star$, $a_r \in \mathbb{F}_{2^m}^\star$, denote by $g_{a_r,b}$ the function $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ and by $g_{a_r,0}$ the function $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$. Since m is odd, the function $g_{a_r,b}$ is constant on each (multiplicative) coset $u\mathbb{F}_{2^m}^\star$ $(u \in U)$ that is, we have:

$$\forall u \in U, \forall y \in \mathbb{F}_{2^m}^\star, g_{a_r,b}(uy) = g_{a_r,b}(u).$$

Using the polar decomposition, the Walsh transform of $f_{a_r,b,c}$ at every $\omega \in \mathbb{F}_{2^n}$ is given by

$$\begin{aligned}
\widehat{\chi_{f_{a_r,b,c}}}(\omega) &= \sum_{x\in\mathbb{F}_{2^n}} \chi\Big(f_{a_r,b,c}(x) + \mathrm{Tr}_1^n(xw)\Big)\\
&= 1 + \sum_{x\in\mathbb{F}_{2^n}^\star} \chi\Big(f_{a_r,b,c}(x) + \mathrm{Tr}_1^n(xw)\Big)\\
&= 1 + \sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big) \sum_{y\in\mathbb{F}_{2^m}^\star} \chi\Big(\mathrm{Tr}_1^m(cy^{2^m+1} + \mathrm{Tr}_m^n(wu)y)\Big)\\
&= 1 + \sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big) \sum_{y\in\mathbb{F}_{2^m}^\star} \chi\Big(\mathrm{Tr}_1^m(c^{\frac{1}{2}}y + \mathrm{Tr}_m^n(wu)y)\Big)\\
&= 1 - \sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big)\\
&+ \sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big) \sum_{y\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m((c^{\frac{1}{2}} + \mathrm{Tr}_m^n(wu))y)\Big)\\
&= 1 - \sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big) + 2^m \sum_{u\in U | c^{\frac{1}{2}} + \mathrm{Tr}_m^n(wu)=0} \chi\Big(g_{a_r,b}(u)\Big).
\end{aligned}$$

Thanks to Lemma 8.1.2, we obtain

$$\widehat{\chi_{f_{a_r,b,c}}}(\omega) \equiv 1 - \sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big) \pmod{2^{m+1}}.$$

But

$$-2^{m+1} < -2^m \leq 1 - \sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big) \leq 2^m + 2 < 2^{m+1}$$

therefore, $f_{a_r,b,c}$ is semi-bent if and only if, $\sum_{u\in U} \chi\Big(g_{a_r,b}(u)\Big) = 1$. We conclude thanks to Corollary 8.1.15. □

Proposition 8.1.18. *([199]) Let $n = 2m$ with m odd. For $r \in R$, $a_r \in \mathbb{F}_{2^m}^\star$, β a primitive element of $\mathbb{F}_4$ and $c \in \mathbb{F}_{2^m}^\star$, let $f_{a_r,\beta,c}$ a function of the form (8.5).*

1. *Let d be a positive integer such that $\gcd(d, \frac{2^m+1}{3}) = 1$. Let $h_{a_r,\beta,c}$ be the function*

$$h_{a_r,\beta,c}(x) = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^m-1)})\, \mathrm{Tr}_1^2(\beta x^{\frac{2^n-1}{3}}) + \mathrm{Tr}_1^m(cx^{2^m+1}).$$

   Then, $h_{a_r,\beta,c}$ is semi-bent if and only if, $f_{a_r,\beta,c}$ is semi-bent.

2. *Suppose $m \not\equiv 3 \pmod 6$. Let d be a positive integer such that $\gcd(d, 2^m+1) = 3$. Let $h_{a_r,1,c}$ be the function*

$$h_{a_r,1,c}(x) = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^m-1)}) + \mathrm{Tr}_1^2(x^{\frac{2^n-1}{3}}) + \mathrm{Tr}_1^m(cx^{2^m+1}).$$

   If $f_{a_r,\beta,c}$ is semi-bent, then $h_{a_r,1,c}$ is semi-bent.

Proof. For two integers r and d, set

$$g_{a_r,0}(x) = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)});$$

$$h_{a_r,0}(x) = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^m-1)}).$$

Proof of 1): according to the proof of Theorem 8.1.17 and relation (8.6), $h_{a_r,\beta,c}$ (Resp. $f_{a_r,\beta,c}$) is semi-bent if and only if $\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) = -1$ (Resp. $\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big) = -1$). Now, the integers $\frac{2^m+1}{3}$ and d are co-prime thus, the mapping $v \mapsto v^d$ is then a permutation of V. Therefore,

$$\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) = \sum_{v\in V}\chi\Big(g_{a_r,0}(v^d)\Big) = \sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big).$$

The result follows.

Proof of 2): the function $f_{a_r,\beta,c}$ is semi-bent thus, according to the proof of Theorem 8.1.17 and relation (8.6), $\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big) = -1$. We have to prove that $h_{a_r,1,c}$ is semi-bent, that is, $\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) - 2\sum_{v\in V}\chi\Big(h_{a_r,0}(\zeta v)\Big) = 1$, according to the proof of Theorem 8.1.17 and relation (8.7). But

$$\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) + \sum_{v\in V}\chi\Big(h_{a_r,0}(\zeta v)\Big) + \sum_{v\in V}\chi\Big(h_{a_r,0}(\zeta^2 v)\Big) = \sum_{u\in U}\chi\Big(h_{a_r,0}(u)\Big)$$

and according to relation (8.10) we have,

$$\sum_{v\in V}\chi\Big(h_{a_r,0}(\zeta v)\Big) = \sum_{v\in V}\chi\Big(h_{a_r,0}(\zeta^2 v)\Big).$$

Therefore, the condition

$$\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) - 2\sum_{v\in V}\chi\Big(h_{a_r,0}(\zeta v)\Big) = 1$$

is equivalent to

$$2\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) - \sum_{u\in U}\chi\Big(h_{a_r,0}(u)\Big) = 1.$$

Now, since $\gcd(d, 2^m+1) = 3$ and the mapping $v \mapsto v^3$ is a permutation when $m \not\equiv 3 \pmod 6$, one has

$$\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) = \sum_{v\in V}\chi\Big(g_{a_r,0}(v^d)\Big) = \sum_{v\in V}\chi\Big(g_{a_r,0}(v^3)\Big) = \sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big).$$

On the other hand, note that (since $\gcd(d, 2^m+1) = 3$)

$$\sum_{u\in U}\chi\Big(h_{a_r,0}(u)\Big) = \sum_{u\in U}\chi\Big(g_{a_r,0}(u^d)\Big) = \sum_{u\in U}\chi\Big(g_{a_r,0}(u^3)\Big) = 3\sum_{v\in V}\chi\Big(g_{a_r,0}(v)\Big).$$

Hence, $2\sum_{v\in V}\chi\Big(h_{a_r,0}(v)\Big) - \sum_{u\in U}\chi\Big(h_{a_r,0}(u)\Big) = -2-(-3) = 1$, proving that $h_{a_r,1,c}$ is semi-bent. □

To conclude this section, some functions in polynomial form in even dimension are considered in this section. We contribute to the knowledge of the class of semi-bent Boolean functions by deriving explicit criteria by means of Kloosterman sums and exponential sums involving Dickson polynomial for determining whether a function expressed as a sum of trace functions is semi-bent or not. Kloosterman sums are used as a very convenient tool to study the semi-bentness property of several functions. In particular, we have showed that the values 0 and 4 of Kloosterman sums defined on $\mathbb{F}_{2^m}$ give rise to semi-bent functions on $\mathbb{F}_{2^n}$. Table 8.2 and Table 8.1 summarize these results.

Table 8.1 – Families of semi-bent functions on $\mathbb{F}_{2^n}$ for $K_m(a) = 0$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$	semi-bent	$K_m(a) = 0$	[199]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ $+ \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{4}+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, m odd	semi-bent	$K_m(a) = 0$	[199]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ $+ \mathrm{Tr}_1^n\left(x^{(2^m-1)3+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$	semi-bent	$K_m(a) = 0$	[199]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$ $+ \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{6}+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, m even	semi-bent	$K_m(a) = 0$	[199]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(\alpha x^{2^m+1}\right)$ $+ \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{\nu-1}-1} x^{(2^m-1)\frac{i}{2^\nu}+1}\right)$; $\gcd(\nu, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_m^n(\alpha) = 1$	semi-bent	$K_m(a) = 0$	[199]

Table 8.2 – Families of semi-bent functions on $\mathbb{F}_{2^n}$ for $K_m(a) = 4$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$; m odd	semi-bent	$K_m(a) = 4$	[199]
$\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m odd and $m \not\equiv 3 \pmod 6$	semi-bent	$K_m(a) = 4$	[199]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$ $+ \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{4}+1}\right)$; m odd	semi-bent	$K_m(a) = 4$	[199]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$ $+ \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{3(2^m-1)+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, m odd	semi-bent	$K_m(a) = 4$	[199]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(\alpha x^{2^m+1}\right)$ $+ \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{\nu-1}-1} x^{(2^m-1)\frac{i}{2^\nu}+1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; $\gcd(\nu, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_m^n(\alpha) = 1$, m odd	semi-bent	$K_m(a) = 4$	[199]

8.2 Semi-bent functions with multiple trace terms and hyperelliptic curves

In chronological order, the results of this section were established before those in Chapter 7. More precisely, in the line of the work of Lisonek [170], we have first established the results of this section in the framework of semi-bent functions before extending them for hyper-bent functions.

This section is in the same spirit as Chapter 7 in which we provide efficient characterizations of the semi-bentness property of several families of Boolean functions in univariate representation with multiple trace terms expressed by means of trace functions via Dillon-like exponents and Niho exponents with even number of variables. To this end, we have precised firstly the connection between the semi-bentness property of such functions and some exponential sums involving Dickson polynomials. Next, we gave a link between the property of semi-bentness and the number of rational points on certain hyperelliptic curves. We exploits the connections between semi-bentness property and binary hyperelliptic curves to produce a polynomial complexity test which is of use in constructing semi-bent functions with multiple trace terms. In the following, we present briefly some results of our study but we do not provide proofs since we have already formulated precisely in this manuscript the connection between exponential sums and cardinalities of hyperelliptic curve in Chapter 7 (see Proposition 11.0.1 and Proposition 11.0.2).

In the following, we consider four infinite classes of functions with multiple trace terms defined on $\mathbb{F}_{2^n}$. We denote by E the set of representatives of the cyclotomic classes modulo 2^n-1 for which each class has full size n. Let $f_{a_r,b,c}$ $f'_{a_r,b}$, $\tilde{f}_{a_r,b',c}$ and $\tilde{f}'_{a_r,b'}$ be the functions defined on $\mathbb{F}_{2^n}$ whose polynomial form is given by (8.11), (8.12), (8.13) and (8.14), respectively.

$$f_{a_r,b,c}(x) := \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}) + \mathrm{Tr}_1^m(cx^{2^m+1}) \tag{8.11}$$

$$f'_{a_r,b}(x) := \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}) + \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(x^{(2^m-1)s+1}\right) \tag{8.12}$$

$$\tilde{f}_{a_r,b',c}(x) := \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^4(b'x^{\frac{2^n-1}{5}}) + \mathrm{Tr}_1^m(cx^{2^m+1}) \tag{8.13}$$

$$\tilde{f}'_{a_r,b'}(x) := \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^4(b'x^{\frac{2^n-1}{5}}) + \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(x^{(2^m-1)s'+1}\right) \tag{8.14}$$

where $R \subseteq E$, $a_r \in \mathbb{F}_{2^m}^\star$, $b \in \mathbb{F}_4^\star$, $b' \in \mathbb{F}_{16}^\star$, $c \in \mathbb{F}_{2^m}^\star$, $s \in \{1/4, 3\}$ and $s' \in \{1/6, 3\}$(the fractions $1/4$ and $1/6$ are understood modulo 2^m+1).

The following statement provides a characterization of the property of semi-bentness for functions of the form (8.11) and (8.12) in terms of cardinalities of hyperelliptic curves.

Theorem 8.2.1. *([200]) Let $n = 2m$ with m odd. Let $b \in \mathbb{F}_4^\star$, β be a primitive element of $\mathbb{F}_4$ and $c \in \mathbb{F}_{2^m}^\star$. Let $f_{a_r,b,c}$ (resp. $f'_{a_r,b}$) be the function defined on $\mathbb{F}_{2^n}$ whose expression is of the form (8.11) (resp. form (8.12)). Let h_{a_r} be the related function defined on $\mathbb{F}_{2^m}$ by $h_{a_r}(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Moreover, let*

$H_{a_r}^{(1)}$, $H_{a_r}^{(2)}$ and $H_{a_r}^{(3)}$ be the (affine) curves defined over $\mathbb{F}_{2^m}$ by

$$H_{a_r}^{(1)} : y^2 + y = \sum_{r\in R} a_r D_r(x),$$
$$H_{a_r}^{(2)} : y^2 + y = \sum_{r\in R} a_r D_r(x + x^3).$$
$$H_{a_r}^{(3)} : y^2 + xy = x + x^2 \sum_{r\in R} a_r D_r(x),$$

a) If β is a primitive element of $\mathbb{F}_4$, then $f_{a_r,\beta,c}$ (resp. $f'_{a_r,\beta}$) is semi-bent if and only if

$$2\#H_{a_r}^{(2)} - \left(\#H_{a_r}^{(1)} + \#H_{a_r}^{(3)}\right) = -3.$$

b) If $b = 1$, then $f_{a_r,1,c}$ (resp. $f'_{a_r,1}$) is semi-bent if and only if

$$4\#H_{a_r}^{(2)} - 5\#H_{a_r}^{(1)} + \#H_{a_r}^{(3)} = 3.$$

The following statement provides a characterization of the property of semi-bentness for functions of the form (8.13) and form (8.14) in terms of cardinalities of hyperelliptic curves.

Theorem 8.2.2. *([200])*

Assume $m := \frac{n}{2} \equiv 2 \pmod 4$. Let $R \subseteq E$ where E is a set of representatives of the cyclotomic classes modulo $2^n - 1$ for which each class has the full size n. Let $b' \in \mathbb{F}_{16}^\star$ and $a_r \in \mathbb{F}_{2^m}^\star$. Let $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) be the function defined on $\mathbb{F}_{2^n}$ whose expression is of the form (8.13) (resp. form (8.14)). Let h_{a_r} be the related function defined on $\mathbb{F}_{2^m}$ by $h_{a_r}(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Moreover, let $H_{a_r}^{(1)}$, $H_{a_r}^{(3)}$, $\tilde{H}_{a_r}{}^{(2)}$ and $\tilde{H}_{a_r}{}^{(3)}$ be the (affine) curves defined over $\mathbb{F}_{2^m}$ by

$$H_{a_r}^{(1)} : y^2 + y = \sum_{r\in R} a_r D_r(x),$$
$$H_{a_r}^{(3)} : y^2 + xy = x + x^2 \sum_{r\in R} a_r D_r(x),$$
$$\tilde{H}_{a_r}{}^{(2)} : y^2 + y = \sum_{r\in R} a_r D_r(x + x^3 + x^5),$$
$$\tilde{H}_{a_r}{}^{(3)} : y^2 + xy = x + x^2 \sum_{r\in R} a_r D_r(x + x^3 + x^5).$$

1. *If Let b' a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b') = 0$, then $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*
$$\#\tilde{H}_{a_r}{}^{(2)} - \#\tilde{H}_{a_r}{}^{(3)} = 5.$$
2. *If $b' = 1$, then $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if*
$$2(\#\tilde{H}_{a_r}{}^{(2)} - \#\tilde{H}_{a_r}{}^{(3)}) - 5(\#H_{a_r}^{(1)} - \#H_{a_r}^{(3)}) = 5.$$
3. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If $b' \in \{\beta, \beta^2, \beta^3\beta^4\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$, then $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*
$$\#\tilde{H}_{a_r}{}^{(2)} - \#\tilde{H}_{a_r}{}^{(3)} + 5(\#H_{a_r}^{(1)} - \#H_{a_r}^{(3)}) = -10.$$

4. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If b' is a primitive element of $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b') = 1$, then $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) if and only if,*

$$3\Big(\#\tilde{H}_{a_r}{}^{(2)} - \#\tilde{H}_{a_r}{}^{(3)}\Big) + 5\Big(\#H_{a_r}^{(3)} - \#H_{a_r}^{(1)}\Big) = -10.$$

5. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If $b' \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4, \beta+\beta^4, \beta^2+\beta^3\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$, then $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*

$$\#\tilde{H}_{a_r}{}^{(2)} - \#\tilde{H}_{a_r}{}^{(3)} = 5.$$

We will not give more details in this section since we have explained in details in Chapter7 the uses of the hyperelliptic curve formalism to reduce computational complexity.

8.3 General constructions of semi-bent functions

In the following, we generalize the constructions given in Section 8.1. More precisely, we prove a key result (Theorem 8.3.1,[45]) which gives rise to the construction of several classes of semi-bent functions in even dimension. First, let recall [82] that a collection $\{E_i,\, i = 1, \ldots, 2^m+1\}$ of vector spaces of dimension $m = n/2$ such that:

1. $E_i \cap E_j = \{0\}$ for every i and j,
2. $\bigcup_{i=1}^{2^m+1} E_i = \mathbb{F}_{2^n}$,

is called a *spread*. The classical example of spread is $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ where U is the multiplicative group $\{u \in \mathbb{F}_{2^n}; u^{2^m+1} = 1\}$.

8.3.1 Characterizations of semi-bent functions

In the next theorem, given a spread $(E_i)_{i=1,\ldots,2^m+1}$, we characterize when a function whose restriction to every E_i^* is affine (i.e. a function equal to the sum of a function whose restriction to every E_i is linear and of a function whose restriction to every E_i^* is constant) is semi-bent:

Theorem 8.3.1. *([45]) Let $m \geq 2$ and $n = 2m$. Let $\{E_i,\, i = 1, \ldots, 2^m+1\}$ be a spread in $\mathbb{F}_{2^n}$ and h a Boolean function whose restriction to every E_i is linear (possibly null). Let S be any subset of $\{1, \ldots, 2^m+1\}$ and $g = \sum_{i\in S} 1_{E_i} \pmod 2$ where 1_{E_i} is the indicator of E_i. Then $g+h$ is semi-bent if and only if g and h are bents.*

We call g a $\mathcal{PS}_{ap}$-like bent function.

Proof. We may without loss of generality assume that $g(0) = 0$, that is, S has even size (otherwise, we replace g by $g+1$). Let us then compute the Walsh Hadamard transform of $g+h$. We have for all $c \in \mathbb{F}_{2^n}$:

$$\begin{aligned}\widehat{\chi_{g+h}}(c) &= \sum_{x\in\mathbb{F}_{2^n}} \chi((g+h)(x) + \mathrm{Tr}_1^n(cx)) \\ &= 1 + \sum_{i=1}^{2^m+1} \sum_{e\in E_i^\star} \chi(g(e) + h(e) + \mathrm{Tr}_1^n(ce))\end{aligned}$$

since $\bigcup_{i=1}^{2^m+1} E_i^\star = \mathbb{F}_{2^n}^\star$ and $E_i^\star \cap E_j^\star = \emptyset$. Let us denote by g_i the value of g on $E_i^\star$, by h_i the restriction of h to E_i and by $I(c)$ the set $\{i \in [1, \ldots, 2^m+1]; \forall e \in E_i,\ h(e) = \mathrm{Tr}_1^n(ce)\}$. We have, for every $c \in \mathbb{F}_{2^n}$:

$$\begin{aligned}\widehat{\chi_{g+h}}(c) &= 1 + \sum_{i=1}^{2^m+1} \chi(g_i) \sum_{e \in E_i^\star} \chi(h_i(e) + \mathrm{Tr}_1^n(ce)) \\ &= 1 - \sum_{i=1}^{2^m+1} \chi(g_i) \\ &\quad + \sum_{i=1}^{2^m+1} \chi(g_i) \sum_{e \in E_i} \chi(h_i(e) + \mathrm{Tr}_1^n(ce)).\end{aligned}$$

Since h_i is linear on E_i, one has $\sum_{e \in E_i} \chi(h_i(e) + \mathrm{Tr}_1^n(ce)) = 2^m$ if $i \in I(c)$ and 0 otherwise. Therefore:

$$\forall c \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{g+h}}(c) = 1 - \sum_{i=1}^{2^m+1} \chi(g_i) + 2^m \sum_{i \in I(c)} \chi(g_i). \tag{8.15}$$

On the other hand, the Walsh Hadamard transform of h is (take $g = 0$ in the preceding calculation) :

$$\widehat{\chi_h}(c) = 2^m(\#I(c) - 1). \tag{8.16}$$

If g is bent then we know that $\sum_{i=1}^{2^m+1} \chi(g_i) = 1$. If h is bent then, according to (8.16), $\#I(c) \in \{0, 2\}$. Hence, if g and h are bent then, $\forall c \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{g+h}}(c) = 2^m \sum_{i \in I(c)} \chi(g_i) \in \{0, \pm 2^{m+1}\}$, proving that $g + h$ is semi-bent.
Conversely, let us assume that $g+h$ is semi-bent and let us show that, necessarily, g and h are bent. According to (8.15), we have $\sum_{i=1}^{2^m+1} \chi(g_i) \equiv 1 \pmod{2^m}$. In other words, $\sum_{i=1}^{2^m+1} \chi(g_i) = 1 + \epsilon 2^m$ with $\epsilon \in \{0, \pm 1\}$. Suppose that $\epsilon \in \{-1, 1\}$, then, for every c, $I(c)$ is non-empty, since if $I(c) = \emptyset$, $\widehat{\chi_{g+h}}(c) = -\epsilon 2^m \notin \{0, \pm 2^{m+1}\}$; this implies that the Walsh Hadamard transform of h is non-negative and we have seen in Section 2.1 (Chapter 2) that h is then linear, say $h(x) = \mathrm{Tr}_1^n(ax)$. We have then, according to (8.16): $\#I(c) = 1$ for $c \neq a$ and $\#I(c) = 2^m + 1$ for $c = a$; thus,

$$\begin{aligned}\widehat{\chi_{g+h}}(a) &= -\epsilon 2^m + 2^m \sum_{i=1}^{2^m+1} \chi(g_i) \\ &= -\epsilon 2^m + 2^m + \epsilon 2^n \\ &= (1 - \epsilon)2^m + \epsilon 2^n \in \{2^n, 2^{m+1} - 2^n\}\end{aligned}$$

a contradiction with the fact that $g + h$ is semi-bent. Therefore, we have $\epsilon = 0$, $\sum_{i=1}^{2^m+1} \chi(g_i) = 1$, which implies that g is bent. Let us now prove that h is bent. One has necessarily $\sum_{i \in I(c)} \chi(g_i) \in \{-2, 0, 2\}$. Thus, $I(c)$ is of even size for every c, which implies that $\widehat{\chi_h}(c)$ is congruent to 2^m modulo 2^{m+1}, which according to Lemma 1 in [25] implies that h is bent (that is, $\#I(c) \in \{0, 2\}$ for every c). □

Remark 8.3.2. *As far as we know, the spread $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ is the only known spread in $\mathbb{F}_{2^n}$, up to linear equivalence.*
There exists an example due for m even to Dillon [82] of a partial spread in $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ which is not included in a spread: $E_\infty = \{0\} \times \{0\} \times \mathbb{F}_{2^{m-1}} \times \mathbb{F}_2$ and $E_a = \{(x, \epsilon, a^2 x + a\,\mathrm{Tr}_1^{m-1}(ax) +$

$a\epsilon, \mathrm{Tr}_1^{m-1}(ax)); (x,\epsilon) \in \mathbb{F}_{2^{m-1}} \times \mathbb{F}_2\}$ *for* $a \in \mathbb{F}_{2^{m-1}}$ *(the corresponding function* g *is quadratic bent).*

We can modify the hypothesis of Theorem 8.3.1 by assuming that we have only a partial spread. We need then to add a condition on the E_i*'s, and we have only a sufficient condition for* $g+h$ *being semi-bent:*
Let g *be a bent function in the* $\mathcal{PS}$ *class, equal to the sum modulo 2 of the indicators of* $l := 2^{m-1}$ *or* $2^{m-1}+1$ *pairwise "disjoint" vector spaces* E_i *having dimension* m*, and* h *a bent function which is linear on each* E_i*. Assume additionally that for every* $c \in \mathbb{F}_{2^n}$ *there exist at most 2 indices* i *such that* $\forall e \in E_i$*,* $h(e) = \mathrm{Tr}_1^n(ce)$*. Then* $g+h$ *is semi-bent. Indeed, we have* $\widehat{\chi_{g+h}}(c) = \widehat{\chi_h}(c) - 2 \sum_{x \in \mathbb{F}_{2^n}/g(x)=1} (-1)^{h(x)+\mathrm{Tr}_1^n(cx)}$ *and therefore, since either* $l = 2^{m-1}$ *and* $g(0) = 0$ *or* $l = 2^{m-1}+1$ *and* $g(0) = 1$*:*

$$\begin{aligned}\widehat{\chi_{g+h}}(c) &= \widehat{\chi_h}(c) - 2\sum_{i=1}^{l}\sum_{e\in E_i}(-1)^{h(e)+\mathrm{Tr}_1^n(ce)} + 2^m \\ &= -2^{m+1}\#\{i=1,\cdots l\,; \forall e \in E_i,\, h(e) = \mathrm{Tr}_1^n(ce)\} \\ &\quad + \widehat{\chi_h}(c) + 2^m\end{aligned}$$

As shown in [24], we have "$\forall e \in E_i; h(e) = \mathrm{Tr}_1^n(ce)$*" for some* i *if and only if* $\widehat{\chi_h}(u) = 2^m$ *for every* $u \in c + E_i^{\perp}$ *which implies in particular that* $\widehat{\chi_h}(c) = 2^m$*. Thus we have:*
- either $\{i = 1,\cdots l\,; \forall e \in E_i,\, h(e) = \mathrm{Tr}_1^n(ce)\} = \emptyset$ *and* $\widehat{\chi_{g+h}}(c) = \widehat{\chi_h}(c) + 2^m \in \{0, 2^{m+1}\}$*;*
- or $\#\{i = 1,\cdots l\,; \forall e \in E_i,\, h(e) = \mathrm{Tr}_1^n(ce)\} \in \{1,2\}$ *and* $\widehat{\chi_{g+h}}(c) \in \{0, -2^{m+1}\}$*. Hence,* $g+h$ *is semi-bent.*

8.3.2 Constructions of semi-bent functions

Constructions in bivariate form

We identify $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with $\mathbb{F}_{2^n}$ by considering an orthonormal basis of the $\mathbb{F}_{2^m}$-vector space $\mathbb{F}_{2^n}$. We consider the vector spaces $E_a = \{(x, ax);\, x \in \mathbb{F}_{2^m}\}$ where $a \in \mathbb{F}_{2^m}$ and $E_\infty = \{(0,y);\, y \in \mathbb{F}_{2^m}\} = \{0\} \times \mathbb{F}_{2^m}$. The bivariate version of the spread $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ is the spread $\{E_a\,;\, a \in \mathbb{F}_{2^m}\} \cup \{E_\infty\}$. It can be directly checked that the E_a's and E_∞ are vector spaces of dimension m and that we have $E_a \cap E_b = \{0\}$ for every pair (a,b) such that $a \neq b$ and $E_\infty \cap E_a = \{0\}$ for every $a \in \mathbb{F}_{2^m}$. Note that any function g in the $\mathcal{PS}_{ap}$ class can be viewed as the indicator of 2^{m-1} or $2^{m-1}+1$ of these vector spaces. Moreover, function h having linear restrictions to the E_a's is necessarily defined as, $x, y \in \mathbb{F}_{2^m}$, $h(x,y) = \mathrm{Tr}_1^m\left(xH\left(\frac{y}{x}\right)\right)$ if $x \neq 0$ and $h(0,y) = \mathrm{Tr}_1^m(\mu y)$ for some mapping H over $\mathbb{F}_{2^m}$ and some $\mu \in \mathbb{F}_{2^m}$. A linear function has bivariate form $\ell(x,y) = \mathrm{Tr}_1^m(cx + c'y)$, where $x, y, c, c' \in \mathbb{F}_{2^m}$ and the set denoted by $I(c)$ in Section 8.3.1 has to be denoted by $I(c,c')$ here. Then for every $(c,c') \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ the set $I(c,c')$ equals $\{a \in \mathbb{F}_{2^m}; \forall x \in \mathbb{F}_{2^m},\, \mathrm{Tr}_1^m(xH(a)) = \mathrm{Tr}_1^m(cx + c'ax)\} = \{a \in \mathbb{F}_{2^m}; H(a) = c + c'a\}$ if $c' \neq \mu$ and $\{a \in \mathbb{F}_{2^m}; H(a) = c + c'a\} \cup \{\infty\}$ if $c' = \mu$. Hence, the sets $I(c,c')$ depend on the pre-image of c by the mapping $H + c'Id$ (where Id denotes the identity map). According to (8.16), the necessary and sufficient condition for h being bent is that, denoting $G(x) = H(x) + \mu x$, then G is a permutation and for every $c' \neq 0$ the function $G(x) + c'x$ is 2-to-1. Such bent functions have been first introduced by Dillon in [82]. He could exhibit in the class of such functions only the example of the function h in Corollary 8.3.3 below. But other examples have been found recently in [44] and lead to Corollary 8.3.5.

Corollary 8.3.3. *([45]) Let g be a function in the $\mathcal{PS}_{ap}$ class (see definition in 4.4.1 (Chapter 4)). Let i be any integer co-prime with m and $h(x,y) = \mathrm{Tr}_1^m(xy^{2^i-1})$. Then the function $g+h$ is semi-bent.*

Remark 8.3.4. *According to [4, Theorem 6], the permutations y^{2^i-1} are the only permutations π such that $x\pi(x)$ is linear.*

Corollary 8.3.5. *([45]) Let g be a function in the $\mathcal{PS}_{ap}$ class. Let h be one of the following functions [44] :*

- $h(x,y) = \mathrm{Tr}_1^m(x^{-5}y^6)$, *$m$ odd;*
- $h(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$, *$m$ odd:*
- $h(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$, $m = 4k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$, $m = 4k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^{2k+1}-2^{3k+1}}y^{2^{2k+1}+2^{3k+1}})$, $m = 4k+1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{2^{3k+1}-2^{2k+1}+2^k}y^{1-2^{3k+1}+2^{2k+1}-2^k})$, $m = 4k+1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^k}y^{2^k} + x^{-(2^k+1)}y^{2^k+2} + x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(y(y^{2^k+1}x^{-(2^k+1)} + y^3x^{-3} + yx^{-1})^{2^{k-1}-1})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}} + x^{\frac{1}{2}}y^{\frac{1}{2}} + x^{\frac{1}{6}}y^{\frac{5}{6}})$, *$m$ odd;*
- $h(x,y) = \mathrm{Tr}_1^m(x[D_{\frac{1}{5}}\left(\frac{y}{x}\right)]^6)$, *$m$ odd, where $D_{\frac{1}{5}}$ is the Dickson polynomial of index $\frac{1}{5}$.*

Then the function $g+h$ is semi-bent.

Remark 8.3.6. *There are more bent functions in bivariate form in [44] whose expression are more complex.*

Constructions in univariate form

We apply now Theorem 8.3.1 to the spread $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ where U is the multiplicative group $\{u \in \mathbb{F}_{2^n}; u^{2^m+1} = 1\}$. In this framework, the functions have to be considered in their univariate form.
- Nonlinear Boolean functions whose restriction to any vector space $u\mathbb{F}_{2^m}$ are linear are sums of Niho power functions, that is (see [93]) of functions of the form:

$$\mathrm{Tr}_1^{o((2^m-1)s+1)}\left(a_s x^{(2^m-1)s+1}\right) \text{ with } 1 \le s \le 2^m$$

We can determine the value of $o((2^m-1)s+1)$ precisely:

Lemma 8.3.7. *([45]) We have $o((2^m-1)s+1) = m$ if $s = 2^{m-1}+1$ (i.e. if $(2^m-1)s+1$ and 2^m+1 are conjugate) and $o((2^m-1)s+1) = n$ otherwise.*

Proof. $2^i((2^m-1)s+1) \equiv (2^m-1)s+1 \pmod{2^n-1}$ is equivalent to $(2^i-1)((2^m-1)s+1) \equiv 0 \pmod{2^n-1}$ and implies $(2^i-1)((2^m-1)s+1) \equiv 0 \pmod{2^m-1}$. The integers 2^m-1 and $(2^m-1)s+1$ being co-prime then, 2^m-1 divides 2^i-1 and then, m divides i. Now, we have $2^m((2^m-1)s+1) \equiv (1-2^m)s+2^m \pmod{2^n-1}$ is congruent to $(2^m-1)s+1$ modulo 2^n-1 if and only if $(2^m-1)(2s-1) \equiv 0 \pmod{2^n-1}$, that is, $s \equiv 2^{m-1}+1 \pmod{2^m+1}$. Therefore, $o((2^m-1)s+1) = m$ if $s = 2^{m-1}+1$ and n otherwise. □

- Some $\mathcal{PS}_{ap}$ functions can be obtained in the form

$$\sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}\left(b_r x^{(2^m-1)r}\right) \text{ where } R \subset \{1,\cdots,2^m\}.$$

Collecting results provided in [93] and [54], we get a direct consequence of Theorem 8.3.1:

Corollary 8.3.8. *Let f be a Boolean function of the form:*

$$f(x) = \mathrm{Tr}_1^m(a_0 x^{2^m+1}) + \sum_{i=1}^{L} \mathrm{Tr}_1^n(a_i x^{(2^m-1)s_i+1}) + \sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}(b_r x^{(2^m-1)r})$$

where L is some non-negative integer, $2 \le s_i \le 2^m$, $s_i \ne 2^{m-1}+1$, $1 \le r \le 2^m$, $a_0 \in \mathbb{F}_{2^m}$, $a_i \in \mathbb{F}_{2^m}$ and $b_r \in \mathbb{F}_{2^{o((2^m-1)r)}}$ (with at least one coefficient $a_i \ne 0$ and one coefficient $b_r \ne 0$). Assume that:
1) the number of roots u in $U := \{x \in \mathbb{F}_{2^n}; x^{2^m+1} = 1\}$ of the equation $\mathrm{Tr}_m^n(cu)+\sum_{i=1}^{L} \mathrm{Tr}_m^n(a_i u^{2s_i-1})+ a_0^{\frac{1}{2}} = 0$ is either 0 or 2 for every $c \in \mathbb{F}_{2^n}$,
2) the sum $\sum_{u\in U} \chi(\sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}(b_r u^r))$ is equal to 1. Then, f is semi-bent.

Proof. Condition 1 is necessary and sufficient to ensure that the Niho part $h(x) := \mathrm{Tr}_1^m(a_0 x^{2^m+1})+ \sum_{i=1}^{L} \mathrm{Tr}_1^n(a_i x^{(2^m-1)s_i+1})$ is bent [93], while condition 2 ensures that the "Dillon" part $g(x) := \sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r}(b_r x^{(2^m-1)r})$ is hyper-bent [54]. □

Remark 8.3.9. *Condition 2 in Corollary 8.3.8 can be reworded by means of Kloosterman sums in particular cases [82], [159], [195], [196], [197] and [198].*

Let us specify some infinite families of semi-bent functions in univariate form. Firstly, we give a list of infinite families containing bent functions defined on $\mathbb{F}_{2^n}$ belonging to the class $\mathcal{PS}_{ap}$; here, $K_m(a) := \sum_{x\in\mathbb{F}_{2^m}} \chi\big(\mathrm{Tr}_1^m(ax+\frac{1}{x})\big)$ denotes the binary Kloosterman sums on $\mathbb{F}_{2^m}$ and $C_m(a,a) := \sum_{x\in\mathbb{F}_{2^m}} \chi\big(\mathrm{Tr}_1^m(ax^3+ax)\big)$ denotes the cubic sums on $\mathbb{F}_{2^m}$:

- $g_1(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)})$; $\gcd(r, 2^m+1) = 1$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 0$ ([54]).
- $g_2(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$; $\gcd(r, 2^m+1) = 1$, $m > 3$ odd, $b \in \mathbb{F}_4^\star$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$ ([197]).
- $g_3(x) = \mathrm{Tr}_1^n(a\zeta^i x^{3(2^m-1)}) + \mathrm{Tr}_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th of unity, $(i,j) \in \{0,1,2\}^2$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$ and $\mathrm{Tr}_1^m(a^{1/3}) = 0$ ([196]).
- $g_4(x) = \mathrm{Tr}_1^n(a\zeta^i x^{3(2^m-1)}) + \mathrm{Tr}_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th of unity, $i \in \{1,2\}$, $j \in \{0,1,2\}$, $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) + C_m(a,a) = 4$ and $\mathrm{Tr}_1^m(a^{1/3}) = 1$ ([196]).

- $g_5(x) = \sum_{i=1}^{2^{m-1}-1} \mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$; $\beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$ ([114]).
- $g_6(x) = \sum_{i=1}^{2^{m-2}-1} \mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$; m odd and $\beta^{(2^m-4)^{-1}} \in \{x \in \mathbb{F}_{2^m}^\star; \mathrm{Tr}_1^m(x) = 0\}$ ([114]).

Secondly, we give a list of known Niho bent functions

- $h_1(x) = \mathrm{Tr}_1^m\left(a_1 x^{2^m+1}\right)$; $a_1 \in \mathbb{F}_{2^m}^\star$
- $h_2(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)3+1}\right)$;
  $a_1 \in \mathbb{F}_{2^n}^\star$, $a_2^{2^m+1} = a_1 + a_1^{2^m} = \beta^5$ for some $\beta \in \mathbb{F}_{2^n}^\star$([93])
- $h_3(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{4}+1}\right)$;
  $a_1 \in \mathbb{F}_{2^n}^\star$ $a_2^{2^m+1} = a_1 + a_1^{2^m}$, m odd [93]
- $h_4(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{6}+1}\right)$; $a_1 \in \mathbb{F}_{2^n}^\star$ $a_2^{2^m+1} = a_1 + a_1^{2^m}$, m even ([93])
- $h_5(x) = \mathrm{Tr}_1^n\left(\alpha x^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} x^{s_i}\right)$, $r > 1$ such that $gcd(r, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha + \alpha^{2^m} = 1$, $s_i = (2^m - 1)\frac{i}{2^r} \pmod{2^m+1} + 1$, $i \in \{1, \cdots, 2^{r-1} - 1\}$ ([160])

We obtain new families in univariate form containing semi-bent functions. Each of them are of algebraic degree m (that is, the maximum degree for a semi-bent function).

Remark 8.3.10. *The question arises of determining whether all these semi-bent functions are extendable to $(n+2)$-variable bent functions. We checked that all the known secondary constructions of bent functions which increase the number of variables by 2 fail to generate such bent functions from g and h. On the other hand, it is difficult to show that a given semi-bent function is the restriction of any bent function (the algebraic degrees of the semi-bent function and of the indicator of its Walsh Hadamard support, for instance, do not help since in both cases they are bounded above by a number which is not smaller for the restriction of a bent function than for a semi-bent function). It is a simple matter to show that a given semi-bent function in n variables, for n even (respectively, for n odd), is the restriction of a semi-bent function (respectively of a bent function) in $n+1$ variables if and only if there exists a semi-bent function f' in n variables whose Walsh Hadamard support $S_{f'} := \{a \in \mathbb{F}_{2^n} / \widehat{\chi_{f'}}(a) \neq 0\}$ is disjoint from S_f, the Walsh Hadamard support of f (note that in the case where n is odd, $\{S_f, S_{f'}\}$ is a partition of $\mathbb{F}_{2^n}$). And a semi-bent function in n variables, for n even, is the restriction of a bent function in $n+2$ variables if and only if it is the restriction of a semi-bent function in $n+1$ variables which is the restriction of a bent function in $n+2$ variables. It is probable that there exist semi-bent functions constructed from Theorem 1 which are the restriction of no bent function in $n+2$ variables, but we were not able to prove it.*

Finally, we give some open problems (Problem 1 has been proposed by Matthew Geoffrey Parker)

Problem 8.3.11. *Show that some semi-bent functions obtained in the previous section are not extendable to $(n+2)$-variable bent functions (or deduce new bent functions from them).*

Problem 8.3.12. *Determine whether there exist spreads which are not linearly equivalent to the spaces $u\mathbb{F}_{2^m}$ and if they exist, deduce related semi-bent functions.*

Problem 8.3.13. *Find semi-bent functions obtained by applying the result of Remark 8.3.2.*

To conclude this section, we show that any Boolean function, in even dimension, equal to the sum of a Boolean function g which is constant on each element of a spread and of a Boolean function h whose restrictions to these elements are all linear, is semi-bent if and only if g and h are both bent. We deduce a large number of infinite classes of semi-bent functions in explicit bivariate (resp. univariate) polynomial form.

Part II

Error Correcting Codes

Chapter 9

Covering radii of binary Reed-Muller codes

Contents

Reed-Muller codes, introduced by D. E. Muller and L. S. Reed in 1954, are one of the best understood families of codes. Except for first-order Reed-Muller codes and for codes of small lengths, their minimum distance is lower than that of BCH codes. But they have very efficient decoding algorithms, they contain nonlinear sub-codes with optimal parameters together with efficient decoding algorithms, and they give a useful framework for the study of Boolean functions in cryptography. Despite the fact that they have been extensively studied for decades by coding theorists, their covering radius is unknown except for Reed-Muller codes of small lengths and for the first-order Reed-Muller code of length 2^n, for n even. The covering radius is the smallest integer ρ such that the spheres of radius ρ centered at the codewords cover the whole space, i.e. the maximum multiplicity of errors that have to be corrected when maximum likelihood decoding is used on a binary symmetric channel. Lower and upper bounds have been proved, but the gap between them is important, and better bounds have to be found. A good reference on covering radius is [68] and a short non-exhaustive list of references on this subject is [69, 130, 131, 186, 230, 239].

Reed-Muller codes can be defined in terms of Boolean functions. Precisely, the binary r^{th}-order Reed-Muller code $\mathcal{RM}(r, n)$ is the set of all binary vectors of length 2^n associated with multivariate binary polynomials $f(x_1, \ldots, x_n)$ of algebraic degree at most r (see *e.g.* [175]). (more precisely, it is the linear code of all binary words of length 2^n corresponding to the last columns of the truth-tables of these functions, see [175]). The Reed-Muller codes are nested

: $\mathcal{RM}(1,n) \subset \mathcal{RM}(2,n) \subset \cdots \subset \mathcal{RM}(n-1,n)$. For every $0 \leq r \leq n-2$, the dual code of $\mathcal{RM}(r,n)$, denoted by $\mathcal{RM}(r,n)^{\perp}$, is the $(n-r-1)$th-order Reed-Muller code with length 2^n.

Recall that $nl_r(f)$ denotes the minimum Hamming distance between a given Boolean function f and all Boolean functions g of degrees at most r. We have:

$$nl_r(f) = 2^{n-1} - \frac{1}{2} \max_{g \in \mathcal{RM}(r,n)} \left| \sum_{x \in F_2^n} (-1)^{f(x)+g(x)} \right| \tag{9.1}$$

The covering radius of $\mathcal{RM}(r,n)$ which plays an important role in error correcting codes, which we denote by $\rho(r,n)$, is defined as the maximum value of $nl_r(f)$ when f ranges the set of Boolean functions in n variables that is

$$\rho(r,n) = \max_{f \in \mathcal{B}_n} \min_{g \in \mathcal{RM}(r,n)} \text{dist}(f,g) \tag{9.2}$$

The covering radii of Reed-Muller codes satisfy the inequality (see [68, 69]):

$$\rho(r,n) \leq \rho(r-1,n-1) + \rho(r,n-1) \tag{9.3}$$

The values of the covering radii of Reed-Muller codes remain unknown except for small lengths and for small or high orders. We recall briefly the only known results about their values. For every positive integer n, $\rho(n,n) = 0$, $\rho(n-1,n) = 1$, $\rho(n-2,n) = 2$ and $\rho(n-3,n) = n+2$ if n is even and $\rho(n-3,n) = n+1$ if n is odd. The covering radius of the first-order Reed-Muller codes is known only for n even and equals in this case $2^{n-1} - 2^{n/2-1}$ while, for n odd, $\rho(1,n)$ is upper bounded by $2^{n-1} - 2^{n/2-1}$ and lower bounded by $2^{n-1} - 2^{(n-1)/2}$ (this value has been slightly improved for $n \geq 15$). Concerning the other values of covering radii of Reed-Muller codes, that is, of Reed-Muller codes of small lengths, we summarize in the Table 9.1 the known values and value brackets for small values of n. We indicate as superscripts the references where these values were obtained.

$r \backslash n$	1	2	3	4	5	6	7	8	9
1	0	1	2	6	12	28	56	120	240-244
2		0	1	2	6	18[1]	40-44[2]	84-100	171-220
3			0	1	2	8	20-23[2]	43-67	111-167
4				0	1	2	8	22-31	58-98
5					0	1	2	10	23-41
6						0	1	2	10
7							0	1	2
8								0	1
9									0

Table 9.1 – Bounds on the covering radii of Reed-Muller codes

Finally, the best known asymptotic upper bound on the covering radius $\rho(r,n)$ of the Reed-Muller code of order r ($r \geq 2$) until 2005, was obtained by Cohen et al. ([68, 69]) :

$$\rho(r,n) \leq 2^{n-1} - \frac{1}{2}(\sqrt{2}+1)^{r-1} \cdot 2^{n/2} + O(n^{r-2}) \tag{9.4}$$

[1] J. Schatz, 1981 [230]
[2] X. D. Hou, 1993 [130]

9.1 New bounds on the covering radii of Reed-Muller codes

We expose briefly in this section our result on the Reed-Muller code of order 2 from which we deduce an upper bound on the covering radii of the Reed-Muller codes of higher orders. The proof of Theorem 9.1.1 is lengthy and will be exposed in Section 9.2

Theorem 9.1.1. *([43]) For every positive integer $n \geq 17$, the covering radius $\rho(2,n)$ of the second-order Reed-Muller code $\mathcal{RM}(2,n)$ is upper bounded by*

$$\left\lfloor 2^{n-1} - \frac{\sqrt{15}}{2} \cdot 2^{\frac{n}{2}} \cdot \left(1 - \frac{122929}{21 \cdot 2^n} - \frac{155582504573}{4410 \cdot 2^{2n}}\right)\right\rfloor \tag{9.5}$$

Concerning the small values of n, we present our upper bound on the covering radius of the second-order Reed-Muller code in the table below, for $n = 10, \ldots, 16$. The first row in this table indicates our upper bound while the second row indicates the upper bound deduced from table 9.1 and inequality (9.3) which we call *recursive bound* :

n	10	11	12	13
Our bound	464	956	1946	3949
Recursive bound	464	960	1961	3977

n	14	15	16
Our bound	7981	16071	32316
Recursive bound	8027	16155	32448

Table 9.2 – Bounds on the covering radii of $\mathcal{RM}(2,n)$ for $10 \leq n \leq 16$

Our upper bound is thus better than the recursive bound whenever $n \geq 10$. A consequence of Theorem 9.1.1 is the following theorem that improves upon the asymptotic bound (9.4) for $r \geq 3$.

Theorem 9.1.2. *([43]) Let r be a positive integer greater than or equal to 2. The covering radius of the Reed-Muller code of order r satisfies asymptotically*

$$\rho(r,n) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{n/2} + O(n^{r-2}) \tag{9.6}$$

Proof. The Theorem is proved by induction on r. Theorem 9.1.1 implies that $\rho(2,n) \leq 2^{n-1} - \sqrt{15} \cdot 2^{\frac{n}{2}-1} + O(1)$. Let (11.12) be valid for $r-1$. Now, inequality (9.3) yields to

$$\begin{aligned}\rho(r,n) &\leq \sum_{j=r}^{n-1} \rho(r-1,j) \\ &\leq \sum_{j=r}^{n-1} \left(2^{j-1} - \sqrt{15} \cdot (1+\sqrt{2})^{r-3} \cdot 2^{\frac{j}{2}-1} + u_j\right)\end{aligned}$$

with $u_j = O(j^{r-3})$. Now

$$\begin{aligned}&\sum_{j=r}^{n-1} \left(2^{j-1} - \sqrt{15} \cdot (1+\sqrt{2})^{r-3} \cdot 2^{\frac{j}{2}-1}\right) \\ &\quad = \frac{2^{n-1} - 2^{r-1}}{2-1} - \frac{\sqrt{15}}{2}(1+\sqrt{2})^{r-3} \cdot \frac{2^{\frac{n}{2}} - 2^{\frac{r}{2}}}{\sqrt{2}-1} \\ &\quad = 2^{n-1} - \frac{\sqrt{15}}{2}(1+\sqrt{2})^{r-2}\, 2^{\frac{n}{2}} + O(1)\end{aligned}$$

On the other hand, since there exists a positive real constant K such that for every positive integer j, $|u_j| \leq Kj^{r-3}$, we have $\left|\sum_{j=r}^{n-1} u_j\right| \leq K \sum_{j=r}^{n-1} j^{r-3} = O(n^{r-2})$. □

9.2 A new upper bound on the covering radii on second-order Reed-Muller codes

Throughout this section, we suppose that n is a positive integer. Let $(f, g) \in \mathcal{B}_n^2$. According to Relation (9.1), we have:

$$\rho(2,n) = 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right| \tag{9.7}$$

For every integer $k \geq 1$ and every $f \in \mathcal{B}_n$, let us set :

$$\mathcal{S}_k(f) := \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k} \tag{9.8}$$

For every $k \geq 1$, $g \in \mathcal{RM}(2,n)$ and $f \in \mathcal{B}_n$, we have :

$$\left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|^{2k+2} \leq \left(\max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right| \right)^2 \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right|^{2k}$$

This implies that, for every integer $k \geq 1$ and every $f \in \mathcal{B}_n$,

$$\mathcal{A}_2(f) := \max_{g \in \mathcal{RM}(2,n)} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right| \geq \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \tag{9.9}$$

We thus get the following upper bound on the covering radius on the second-order Reed-Muller code :

$$\forall k \geq, \quad \rho(2,n) \leq 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \tag{9.10}$$

The covering radius $\rho(2,n)$ being an integer, we thus have, for every integer $k \geq 1$,

$$\rho(2,n) \leq \rho_k(2,n) = \left\lfloor 2^{n-1} - \frac{1}{2} \min_{f \in \mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \right\rfloor \tag{9.11}$$

Lemma 9.2.1 below shows that the sequence $(\rho_k(2,n))_{k \geq 1}$ admits $\rho(2,n)$ as a limit.

Lemma 9.2.1. *([43]) The integer sequence $(\rho_k(2,n))_{k \geq 1}$ is decreasing. Moreover there exists a positive integer k such that $\rho_k(2,n) = \rho(2,n)$.*

Proof.

1. Cauchy-Schwartz's inequality yields to

$$\forall f \in \mathcal{B}_n, \forall k \geq 1, \quad \mathcal{S}_{k+1}^2(f) \leq \mathcal{S}_k(f)\, \mathcal{S}_{k+2}(f)$$

This implies that the sequence $\left(\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}\right)_{k\geq 1}$ is increasing for every Boolean function $f \in \mathcal{B}_n$ and therefore the sequence $\left(\min_{f\in\mathcal{B}_n} \frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}\right)_{k\geq 1}$ is increasing too. This proves that the sequence $(\rho_k(2,n))_{k\geq 1}$ is decreasing.

2. Given a sequence of non-negative integers λ_i, the ratio $\frac{\sum_i \lambda_i^{k+1}}{\sum_i \lambda_i^k}$ tends to $\max_i \lambda_i$ when k tends to infinity. Indeed, $\sum_i \lambda_i^p$ is equivalent to $N\Big(\max_i \lambda_i\Big)^p$ as p tends to infinity where N is the cardinality of $\{j \mid \lambda_j = \max_i \lambda_i\}$. Therefore $\frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$ converges to $\frac{1}{2}\mathcal{A}_2(f)$ as k tends to infinity. Now, according to (9.9), we have

$$\frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \leq \left\lceil \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \right\rceil \leq \frac{1}{2}\mathcal{A}_2(f)$$

We have used the fact that $\frac{1}{2}\mathcal{A}_2(f)$ is an integer. This implies that, for every Boolean function $f \in \mathcal{B}_n$, there exists a positive integer k_f such that, $\left\lceil \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \right\rceil = \frac{1}{2}\mathcal{A}_2(f)$ provided that $k \geq \mathrm{k}_f$. Therefore, whenever $k \geq \max_{f\in\mathcal{B}_n} \mathrm{k}_f$, we have $\min_{f\in\mathcal{B}_n} \left\lceil \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \right\rceil = \frac{1}{2}\min_{f\in\mathcal{B}_n} \mathcal{A}_2(f)$. This implies that $\rho_k(2,n) = 2^{n-1} - \min_{f\in\mathcal{B}_n} \left\lceil \frac{1}{2}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \right\rceil = 2^{n-1} - \frac{1}{2}\min_{f\in\mathcal{B}_n} \mathcal{A}_2(f) = \rho(2,n)$ whenever $k \geq \max_{f\in\mathcal{B}_n} \mathrm{k}_f$.

□

Lemma 9.2.1 shows that, the greater we take the value of k, the better the lower bound obtained with (9.9) should be. Unfortunately, we will be brought to restrict the choice of k and and we shall get only a bound.

According to (9.11), the problem of getting an upper bound on $\rho(2,n)$ is equivalent to searching a lower bound on $\min_{f\in\mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$. The remaining of the section is entirely devoted to establish such a lower bound. The proof being rather lengthy, we structure its presentation by splitting it in independent subsections.

9.2.1 A decomposition of the power sums $\mathcal{S}_k(f)$ in character sums

This subsection is entirely devoted to stating a decomposition of the power sums $\mathcal{S}_k(f)$ into character sums involving characters of $\mathcal{B}_n$. To this aim, we start by rewriting the power sums $\mathcal{S}_k(f)$. We first introduce a notation that we shall use in this lemma and in the sequel : given two n-variable Boolean functions f and g, we denote by $\langle f, g\rangle$ the sum $\sum_{x\in\mathbb{F}_2^n} f(x)g(x)$.

Lemma 9.2.2. *([43]) Let f be any n-variable Boolean function. Then, for every positive integer k, we have*

$$\mathcal{S}_k(f) \;=\; \#\,\mathcal{RM}(2,n) \sum_{(x_1,\cdots,x_{2k})\in\mathcal{U}_k} (-1)^{\langle f, \sum_{i=1}^{2k} 1_{x_i}\rangle}$$

where $\mathcal{U}_k$ denotes the subset of $(\mathbb{F}_2^n)^{2k}$ formed with all the $2k$-tuples $(x_1,\cdots,x_{2k})$ such that the Boolean function $\sum_{i=1}^{2k} 1_{x_i}$ belongs to $\mathcal{RM}(n-3,n)$ (here, 1_x denotes the Boolean functions in n variables whose support is the singleton $\{x\}$, $x \in \mathbb{F}_2^n$)

Proof. Expanding the power terms $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}\right)^{2k}$ in (9.8) yields to :

$$\mathcal{S}_k(f) = \sum_{x_1,\ldots,x_{2k}\in\mathbb{F}_2^n}(-1)^{\sum_{i=1}^{2k} f(x_i)}\left(\sum_{g\in\mathcal{RM}(2,n)}(-1)^{\sum_{i=1}^{2k} g(x_i)}\right)$$

The mapping $g \mapsto g(x_1)+\cdots+g(x_{2k}) = \langle g, 1_{x_1}+\cdots+1_{x_{2k}}\rangle$ being linear over the Reed-Muller code of order 2 and this code being linear, the sum of $(-1)^{g(x_1)+\cdots+g(x_{2k})}$ when g ranges over the Reed-Muller code of order 2 either is null or equals $\#\,\mathcal{RM}(2,n)$. More precisely, this sum equals to $\#\,\mathcal{RM}(2,n)$ if the Boolean function $1_{x_1}+\cdots+1_{x_{2k}}$ belongs to the dual code $\mathcal{RM}(2,n)^\perp$ of the second-order Reed-Muller code, that is the Reed-Muller code of order $n-3$, and is null otherwise. □

The next step is to use Lemma 9.2.2 to get a decomposition in character sums of the power sums $\mathcal{S}_k(f)$ for all positive integers k and all Boolean functions $f \in \mathcal{B}_n$. For that,we introduce additional notation for convenience.

Definition 9.2.3. *Let k be a positive integer. We let D_k be the number of ways of choosing a $2k$-tuple $(x_1,\cdots,x_{2k})$ such that $\sum_{i=1}^{2k} 1_{x_i}$ equals the null codeword. More generally, given a positive integer w, we let $N_k^{(w)}$ be the number of ways of choosing a $2k$-tuple $(x_1,\cdots,x_{2k})$ constituting (taking into account the order) an arbitrary function of Hamming weight w. Finally, we let $M_f^{(w)}$ be the character sum of $(-1)^{\langle f,g\rangle}$ when g ranges over the subset of those codewords of $\mathcal{RM}(n-3,n)$ of Hamming weight w .*

Remark 9.2.4. *We adopt the convention $M_f^{(w)} = 0$ if there is no codeword of Hamming weight w in $\mathcal{RM}(n-3,n)$*

We then prove

Proposition 9.2.5. *([43]) Let f be an arbitrary Boolean function of $\mathcal{B}_n$. Then*

$$\begin{aligned}
&\mathcal{S}_k(f) = \#\,\mathcal{RM}(2,n)\,D_k \quad \text{if } k=1,2,3\\
&\mathcal{S}_k(f) = \#\,\mathcal{RM}(2,n)\left(D_k + N_k^{(8)}M_f^{(8)}\right) \text{ if } k=4,5\\
&\mathcal{S}_k(f) =\\
&\#\,\mathcal{RM}(2,n)\left(D_k + N_k^{(8)}M_f^{(8)} + \sum_{w=6}^{k} N_k^{(2w)}M_f^{(2w)}\right),\\
&\qquad \text{if } k\geq 6
\end{aligned} \tag{9.12}$$

Proof. Let $f \in \mathcal{B}_n$. According to Lemma 9.2.2, we have, for all positive integer k,

$$\begin{aligned}
\mathcal{S}_k(f) &= \#\,\mathcal{RM}(2,n) \sum_{(x_1,\cdots,x_{2k})\in\mathcal{U}_k}(-1)^{\langle f,\sum_{i=1}^{2k}1_{x_i}\rangle}\\
&= \#\,\mathcal{RM}(2,n)\left(D_k + \sum_{g\in\mathcal{RM}(n-3,n)\setminus\{0\}}\#\mathcal{N}_g\,(-1)^{\langle f,g\rangle}\right)
\end{aligned}$$

where $\mathcal{N}_g$ denotes the set of all the $2k$-tuples $(x_1,\ldots,x_{2k})$ of vectors of $\mathbb{F}_2^n$ such that $\sum_{i=1}^{2k}1_{x_i} = g$. Let σ be a permutation of $\mathbb{F}_2^n$. Now, clearly, the map from $(\mathbb{F}_2^n)^{2k}$ to itself which maps $(x_1,\ldots,x_{2k})$

to $(\sigma(x_1), \ldots, \sigma(x_{2k}))$ is one-to-one and maps $\mathcal{N}_g$ to $\mathcal{N}_h$ where h is the Boolean function defined as $h(x) = g(\sigma^{-1}(x))$. This implies that $\#\mathcal{N}_g = \#\mathcal{N}_h = N_k^{(w)}$ whenever $\mathrm{wt}(g) = \mathrm{wt}(h) = w$. Therefore

$$\mathcal{S}_k(f) = \#\,\mathcal{RM}(2,n)\left(D_k + \sum_{w=1}^{2k} N_k^{(w)}\left(\sum_{\substack{g\in\mathcal{RM}(n-3,n)\\ \mathrm{wt}(g)=w}} (-1)^{\langle f,g\rangle}\right)\right)$$

The proof is complete by recalling that

1. The Hamming weight of any codeword of $\mathcal{RM}(n-3,n)$ is even
2. The Reed-Muller code of order $n-3$ has minimum distance 8 and there is no element of Hamming weight 10 [145].

□

Proposition 9.2.5 states that, for any Boolean function $f \in \mathcal{B}_n$,

$$\begin{aligned}
\frac{\mathcal{S}_2(f)}{\mathcal{S}_1(f)} &= \frac{D_2}{D_1}\\
\frac{\mathcal{S}_3(f)}{\mathcal{S}_2(f)} &= \frac{D_3}{D_2}\\
\frac{\mathcal{S}_4(f)}{\mathcal{S}_3(f)} &= \frac{D_4 + N_4^{(8)} M_f^{(8)}}{D_3}\\
\frac{\mathcal{S}_5(f)}{\mathcal{S}_4(f)} &= \frac{D_5 + N_5^{(8)} M_f^{(8)}}{D_4 + N_4^{(8)} M_f^{(8)}}\\
\frac{\mathcal{S}_6(f)}{\mathcal{S}_5(f)} &= \frac{D_6 + N_6^{(8)} M_f^{(8)} + N_6^{(12)} M_f^{(12)}}{D_5 + N_5^{(8)} M_f^{(8)}}\\
\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} &= \frac{D_{k+1} + N_{k+1}^{(8)} M_f^{(8)} + \sum_{w=6}^{k+1} N_{k+1}^{(2w)} M_f^{(2w)}}{D_k + N_k^{(8)} M_f^{(8)} + \sum_{w=6}^{k} N_k^{(2w)} M_f^{(2w)}}\\
&\qquad \text{for } k \geq 6
\end{aligned}$$

Remark 9.2.6. *According to (9.11), we have, for every positive integer k, $\rho(2,n) \leq \left\lfloor 2^{n-1} - \frac{1}{2}\min_{f\in\mathcal{B}_n}\sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}\right\rfloor$. Since $D_1 = 2^n$, $D_2 = 3\cdot 2^{2n} - 2\cdot 2^n$ and $D_3 = 15\cdot 2^{3n} - 30\cdot 2^{2n} + 16\cdot 2^n$, we deduce two upper bounds by setting $k = 1$ and $k = 2$: $\rho(2,n) \leq \left\lfloor 2^{n-1} - \frac{1}{2}\sqrt{3\cdot 2^n - 2}\right\rfloor$ and $\rho(2,n) \leq \left\lfloor 2^{n-1} - \frac{1}{2}\sqrt{\frac{15\cdot 2^{2n} - 30\cdot 2^n + 16}{3\cdot 2^n - 2}}\right\rfloor$. The first upper bound does not improve upon the upper bound on the covering radius of $\mathcal{RM}(2,n)$ presented in [68] while the second one does.*

9.2.2 The values of $N_k^{(2w)}$

In the decomposition of $\mathcal{S}_k(f)$, the numbers D_k and $N_k^{(2w)}$ can be computed for all positive integers k and w. We introduce some notation to state their expressions. Given a mapping A from $\mathbb{R}$ to itself, we denote by $\left[z^k\right] A(z)$ the coefficient of $\frac{z^k}{k!}$ in the Taylor series expansion of A at $z = 0$.

Lemma 9.2.7. *([43]) For every positive integer k and every positive integer w, we have*

$$D_k = [z^{2k}] \cosh^{2^n}(z)$$
$$N_k^{(2w)} = [z^{2k}] \tanh^{2w} \cosh^{2^n}(z)$$

Proof.

1. By definition, D_k equals the number of ways of choosing a $2k$-tuple $(x_1, \ldots, x_{2k})$ of vectors of $\mathbb{F}_2^n$ such that $\sum_{i=1}^{2k} 1_{x_i}$ equals the null codeword. Clearly, this holds if and only if we can constitute k pairs of identical elements with $x_1, \ldots, x_{2k}$. These pairs are not necessarily pairwise distinct. More precisely, these vectors $x_1, \ldots, x_{2k}$ constitute a *multiset* (*i.e.* a set-like object for which repeated elements are considered but in which the order is ignored; the number of times that each element appears is called the *multiplicity*). Assume that this multiset is constituted with s pairwise distinct elements with multiplicities $q_1, \ldots, q_s$ $(1 \leq s \leq 2^n)$. These multiplicities q_i are necessarily even in order to be able to constitute pairs of identical elements and form a *composition* of $2k$, *i.e.* an ordered tuple of positive integers with total sum $2k$. Set $p_i = \frac{q_i}{2}$ for every $i \in \{1, \ldots, s\}$. Thus

$$D_k = \sum_{s=1}^{\min(k,2^n)} \binom{2^n}{s} \sum_{p_1+\cdots+p_s=k} \frac{(2k)!}{\prod_{i=1}^{s}(2p_i)!}$$

where the $\sum_{p_1+\cdots+p_s=k}$ denotes the sum over all the compositions of k of length s. Let us now compute the generating series of the integer sequence $(D_k)_{k\in\mathbb{N}}$

$$\begin{aligned}
\sum_{k=1}^{+\infty} D_k \frac{z^{2k}}{2k!} &= \sum_{k=1}^{+\infty} \sum_{s=1}^{\min(k,2^n)} \binom{2^n}{s} \sum_{p_1+\cdots+p_s=k} \prod_{i=1}^{s} \frac{z^{2p_i}}{(2p_i)!} \\
&= \sum_{s=1}^{2^n} \binom{2^n}{s} \left(\sum_{k=s}^{+\infty} \sum_{p_1+\cdots+p_s=k} \prod_{i=1}^{s} \frac{z^{2p_i}}{(2p_i)!} \right) \\
&= \sum_{s=1}^{2^n} \binom{2^n}{s} \left(\sum_{p=1}^{+\infty} \frac{z^{2p}}{(2p)!} \right)^s \\
&= \sum_{s=1}^{2^n} \binom{2^n}{s} (\cosh(z) - 1)^s \\
&= \cosh^{2^n}(z) - 1
\end{aligned}$$

2. By definition, $N_k^{(2w)}$ equals the number of ways of choosing a $2k$-tuple $(x_1, \cdots, x_{2k})$ constituting an arbitrary function g (of $\mathcal{RM}(n-3, n)$) of Hamming weight $2w$. Clearly, in the particular case where $w = k$, one has $N_k^{(2k)} = (2k)!$ (the number of permutations of $\mathrm{supp}(g)$). On the other hand, when $w < k$, a $2k$-tuple $(x_1, \ldots, x_{2k})$ such that $\sum_{i=1}^{2k} 1_{x_i} = g$ must be constituted of $k - w$ pairs of identical elements and the $2w$ other elements are the elements of $\mathrm{supp}(g)$. Moreover, the elements of such $2k$-tuples constitute a multiset of length $2k$ formed with all the elements of $\mathrm{supp}(g)$ and some other pairwise distinct elements of $\mathbb{F}_2^n \setminus \mathrm{supp}(g)$ (if necessary). The multiplicity of an element of $\mathrm{supp}(g)$ is necessarily odd while the multiplicity of the other elements of the multiset is necessarily even. Moreover, in order to be able to constitute $k - w$ pairs of identical elements, these multiplicities must

constitute a composition of $2k$. Hence,
- denoting by r the number of those elements of $\mathrm{supp}(g)$ whose multiplicities are greater than 1 and denoting by $2q_1+1,\ldots,2q_r+1$ these multiplicities,
- denoting by s the number of those elements chosen outside $\mathrm{supp}(g)$ and denoting by $2p_1,\ldots,2p_s$ their multiplicities, $N_k^{(2w)}$ equals:

$$\sum_{\substack{1\leq r+s\leq k-w\\0\leq r\leq 2w\\0\leq s\leq 2^n-2w}}\binom{2w}{r}\binom{2^n-2w}{s}\times\sum_{w+p_1+\cdots+p_s+q_1+\cdots+q_r=k}\frac{(2k)!}{\prod_{i=1}^r(2q_i+1)!\prod_{i=1}^s(2p_i)!}.$$

where the sum $\sum_{w+p_1+\cdots+p_s+q_1+\cdots+q_r=k}$ denotes the sum over the set $\bigcup_{0\leq u\leq k-w}E_u$ and where E_u is the set formed with all the $(r+s)$th-tuples $\{(p_1,\ldots,p_s,q_1,\ldots,q_r)\in(\mathbb{N}^\star)^{s+r}$ such that $(p_1,\ldots,p_s)$ is a composition of u and $(q_1,\ldots,q_r)$ is a composition of $k-w-u$. Let us now compute the generating series of the integer sequence $(N_k^{(2w)})_{k\in\mathbb{N}}$:

$$\begin{aligned}
&\sum_{k=w}^{+\infty}2wk\frac{z^{2k}}{(2k)!}\\
&=z^{2w}\left[1+\sum_{\substack{0\leq r\leq 2w\\0\leq s\leq 2^n-2w\\r+s\geq 1}}\binom{2w}{r}\binom{2^n-2w}{s}\right.\\
&\quad\times\sum_{k=r+s+w}^{+\infty}\sum_{\substack{p_i,q_i\geq 1\\\sum_{i=1}^s p_i+\sum_{i=1}^r q_i=k-w}}\prod_{i=1}^s\frac{z^{2p_i}}{(2p_i)!}\\
&\qquad\left.\times\prod_{i=1}^r\frac{z^{2q_i}}{(2q_i+1)!}\right]\\
&=z^{2w}+\sum_{\substack{0\leq r\leq 2w\\0\leq s\leq 2^n-2w\\r+s\geq 1}}z^{2w-r}\left(\sum_{p=1}^{+\infty}\frac{z^{2p}}{(2p)!}\right)^s\\
&\qquad\times\left(\sum_{q=1}^{+\infty}\frac{z^{2q+1}}{(2q+1)!}\right)^r\\
&=z^{2w}+\sum_{\substack{0\leq r\leq 2w\\0\leq s\leq 2^n-2w\\r+s\geq 1}}\binom{2w}{r}\binom{2^n-2w}{s}z^{2w-r}\\
&\qquad\times(\cosh(z)-1)^s(\sinh(z)-z)^r\\
&=\sum_{r=0}^{2w}\sum_{s=0}^{2^n-2w}\binom{2w}{r}\binom{2^n-2w}{s}z^{2w-r}\\
&\qquad\times(\cosh(z)-1)^s(\sinh(z)-z)^r\\
&=(\cosh(z))^{2^n-2w}(\sinh(z))^{2w}
\end{aligned}$$

□

Corollary 9.2.8. *([43]) We have :*
$D_4 = 588 \cdot 2^{2n} - 272 \cdot 2^n - 420 \cdot 2^{3n} + 105 \cdot 2^{4n}$

$D_5 = 7936 \cdot 2^n - 18960 \cdot 2^{2n} + 16380 \cdot 2^{3n} - 6300 \cdot 2^{4n} + 945 \cdot 2^{5n}$

$D_6 = 911328 \cdot 2^{2n} - 353792 \cdot 2^n - 893640 \cdot 2^{3n} + 429660 \cdot 2^{4n} - 103950 \cdot 2^{5n} + 10395 \cdot 2^{6n}$

$D_7 = 22368256 \cdot 2^n - 61152000 \cdot 2^{2n} + 65825760 \cdot 2^{3n} - 36636600 \cdot 2^{4n} + 11351340 \cdot 2^{5n} - 1891890 \cdot 2^{6n} + 135135 \cdot 2^{7n}$

$D_8 = 5464904448 \cdot 2^{2n} - 1903757312 \cdot 2^n - 6327135360 \cdot 2^{3n} + 3918554640 \cdot 2^{4n} - 1427025600 \cdot 2^{5n} + 310269960 \cdot 2^{6n} - 37837800 \cdot 2^{7n} + 2027025 \cdot 2^{8n}$

$N_4^{(8)} = 8!,\ N_5^{(8)} = 8!\,(45 \cdot 2^n - 240)$

$N_6^{(8)} = 8!\,\big(1485 \cdot 2^{2n} - 16830 \cdot 2^n + 49632\big),\ N_6^{(12)} = 12!$

$N_7^{(8)} = 8!\Big(5045040\, 2^n - 810810 \cdot 2^{2n} + 45045 \cdot 2^{3n} - 10799360\Big)$

$N_7^{(12)} = 12!\,(91 \cdot 2^n - 728),\ N_7^{(14)} = 14!$

$N_8^{(8)} = 8!\Big(336215880 \cdot 2^{2n} - 1510835040 \cdot 2^n - 34234200 \cdot 2^{3n} + 1351350 \cdot 2^{4n} + 2611834368\Big)$

$N_8^{(12)} = 12!\,\big(5460 \cdot 2^{2\,n} - 91000 \cdot 2^n + 390208\big)$

$N_8^{(14)} = 14!\,(120 \cdot 2^n - 1120),\ N_8^{(16)} = 16!$

9.2.3 Lower bounds on $M_f^{(2w)}$

Throughout this subsection, $\mathcal{A}_\ell$ denotes the set of all ℓ-dimensional flats in $\mathbb{F}_2^n$ while $\mathcal{E}_\ell$ denotes the set of all ℓ-dimensional spaces in $\mathbb{F}_2^n$.

We recall that we are searching to establish a lower bound on $\min_{f\in\mathcal{B}_n} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$. Remark 9.2.6 leads us to consider $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$ for $k \geq 3$ and to search to establish a lower bound on $\min_{f\in\mathcal{B}_n} \frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$.

We need to determine a lower bound on $\min_{f\in\mathcal{B}_n} M_f^{(2w)}$. We for that use the characterizations, due to Kasami and *al* [145, 243], of the elements of Reed-Muller codes. Indeed, the codewords of $\mathcal{RM}(r,n)$, $0 \leq r \leq n-1$, have been characterized and enumerated by Kasami and *al* up (strictly) to $2,5 \cdot d_{min}$ (where $d_{min} = 2^{n-r}$ denotes the minimal distance of $\mathcal{RM}(r,n)$). This corresponds in our case to the codewords of $\mathcal{RM}(n-3,n)$ whose Hamming weight ranges from 8 to 18. Thus, we are restricted to consider the cases where $k \leq 9$ in our calculations. Unfortunately, we have to restrict more the values of k because we were not able to deduce any significant lower bounds from the results of Kasami and *al* when $k = 9$. We therefore restrict k to be less than or equal to 8 from now on. We now briefly recall the characterizations and the numbers of codewords of $\mathcal{RM}(n-3,n)$ whose Hamming weight ranges from 8 to 16. Below, $\begin{bmatrix} n \\ p \end{bmatrix}$ denotes the *gaussian coefficient* $\frac{\prod_{i=0}^{p-1}(2^n-2^i)}{\prod_{i=0}^{p-1}(2^p-2^i)}$.

1. The elements of Hamming weight 8 are the indicators of 3-dimensional flats (i.e. affine subspaces) of F_2^n. The number of these codewords equals hence $2^{n-3}\begin{bmatrix} n \\ 3 \end{bmatrix}$.

2. [145, Theorem 1, (2)] The codewords of weight 12 are the indicators of those sets of the form $(A_1 \cup A_2) \setminus (A_1 \cap A_2)$ where A_1 and A_2 are two 3-dimensional flats whose intersection has dimension 1. The number of these codewords is $2^{n+2} \cdot \frac{\prod_{i=0}^{n-2}(2^{n-i}-1)}{\prod_{i=0}^{n-6}(2^{n-5-i}-1)\cdot\prod_{i=0}^{1}(4^{i+1}-1)}$, see $|Q^{(2)}_{n,n-5,2}|$ in [145, p. 759]. From this, we can deduce that the codewords of Hamming weight 12 have a unique representation as the indicators of sets $(A_1 \cup A_2) \setminus (A_1 \cap A_2)$. This can be proved in a simple original way, that we give for self-completeness. Suppose that A_1, A_2, B_1 and B_2 are four 3-dimensional flats such that $(A_1 \cup A_2) \setminus (A_1 \cap A_2) = (B_1 \cup B_2) \setminus (B_1 \cap B_2)$ and $\dim(A_1 \cap A_2) = \dim(B_1 \cap B_2) = 1$. Write these flats as $A_1 = u + U + E_1$, $A_2 = u + U + E_2$, $B_1 = v + V + F_1$ and $B_2 = v + V + F_2$, with $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, $(U, V) \in \mathcal{E}_1^2$, and $(E_1, E_2, F_1, F_2) \in \mathcal{E}_2^4$ such that $E_1 \cap E_2 = \{0\}$ and $F_1 \cap F_2 = \{0\}$. The Fourier transform at any point a of the indicator of $(A_1 \cup A_2) \setminus (A_1 \cap A_2)$, that is, of the function $1_{A_1} + 1_{A_2} - 2 \cdot 1_{A_1 \cap A_2}$, equals $(-1)^{u\cdot a}[8 \cdot 1_{(U+E_1)^\perp}(a) + 8 \cdot 1_{(U+E_2)^\perp}(a) - 4 \cdot 1_{U^\perp}(a)]$. This Fourier transform does not vanish on $U^\perp$ and is null otherwise. Similarly, we get that this Fourier transform does not vanish on $V^\perp$ and is null otherwise. Whence $U^\perp = V^\perp$ and thus $U = V$. We also deduce that, for every $a \in U^\perp$, we have $u \cdot a = v \cdot a$, that is, $u + v \in U$. We finally have to check that if $E_1 \cup E_2 = F_1 \cup F_2$ then we have $E_1 = F_1$ and $E_2 = F_2$ or $E_1 = F_2$ and $E_2 = F_1$. We deduce from $E_1 \cup E_2 = F_1 \cup F_2$ that $E_1 = (F_1 \cap E_1) \cup (F_2 \cap E_1)$. Now the union $(F_1 \cap E_1) \cup (F_2 \cap E_1)$ can be a vector space if and only if two cases hold : firstly, $F_1 \cap E_1 = \{0\}$ or $F_2 \cap E_1 = \{0\}$; suppose $F_1 \cap E_1 = \{0\}$; the equality $E_1 = F_2 \cap E_1$ implies that $F_2 = E_1$ from which we deduce that $F_1 = E_2$; likewise, we deduce from the condition $F_2 \cap E_1 = \{0\}$ that $F_1 = E_1$ and $F_2 = E_2$; secondly, $F_1 \cap E_1 \subset F_2 \cap E_1$ or $F_2 \cap E_1 \subset F_1 \cap E_1$ contradicting $F_1 \cap F_2 = \{0\}$.

3. [145, Theorem 1, (1)] The codewords of Hamming weight 14 are the indicators of those sets of the form $(A_1 \cup A_2) \setminus (A_1 \cap A_2)$ where A_1 and A_2 are two 3-dimensional flats whose intersection is a singleton. The number of these codewords equals $2^{n+8} \cdot \frac{\prod_{i=0}^{n-1}(2^{n-i}-1)}{\prod_{i=0}^{n-7}(2^{n-6-i}-1)\cdot\prod_{i=0}^{2}(2^{3-i}-1)^2}$, see $|Q^{(1)}_{n,n-6,3}|$ in [145, p. 759]. These codewords have a unique representation too. Indeed, suppose that $(A_1 \cup A_2) \setminus (A_1 \cap A_2) = (B_1 \cup B_2) \setminus (B_1 \cap B_2)$ with $A_1 \cap A_2 = \{u\}$ and $B_1 \cap B_2 = \{v\}$. Writing $A_1 = u + E_1$, $A_2 = u + E_2$, $B_1 = v + F_1$ and $B_2 = v + F_2$, we must have that $u + (E_1 \cup E_2) = v + (F_1 \cup F_2)$. The same arguments as above show that $u = v$ and that $E_1 \cup E_2 = F_1 \cup F_2$ is possible only if $E_1 = F_1$ and $E_2 = F_2$ or $E_1 = F_2$ and $E_2 = F_1$.

4. [243, Table I, (11)] The codewords of Hamming weight 16 are the indicators of those sets of the form $A_1 \cup A_2$ where A_1 and A_2 are two disjoint 3-dimensional flats. The number of these codewords equals $\begin{bmatrix} n \\ 4 \end{bmatrix} 2^{n-4} + 18228 \begin{bmatrix} n \\ 5 \end{bmatrix} 2^{n-4} + 888615 \begin{bmatrix} n \\ 6 \end{bmatrix} 2^{n+2} + 17964531 \begin{bmatrix} n \\ 7 \end{bmatrix} 2^{n+7} + \left(\sum_{k=5}^{n-3} \frac{\beta_{k+3}\begin{bmatrix} n \\ k+3 \end{bmatrix} 2^{n-k+k^2-4}}{\beta_{k-1}^2}\right)$ where $\beta_m = \prod_{i=0}^{m-1}(2^{m-i}-1)$, see $N_{m,r,2^{m-r+1}}$ in [243, p.392 (a)]

Remark 9.2.9. *Although the number of codewords of Hamming weight $2w$ is known for $w \leq 8$, the lower bound on the character sums $M_f^{(2w)}$ this permits to derive gives no real information because this number is too large.*

Using the characterizations above, we prove

Proposition 9.2.10. *([43]) For every Boolean function f in n variables, we have*

$$\begin{aligned}
&1.\ \ M_f^{(8)} \geq -\frac{2^n(2^n-1)(2^n-2)}{336}\\
&2.\ M_f^{(12)} \geq -\frac{2^n(2^n-1)(2^n-2)(2^n-4)(3\cdot 2^n-20)}{384}\\
&3.\ M_f^{(14)} \geq -\frac{2^n\,(2^n-1)\,(2^n-2)\,(2^n-4)}{8064}\\
&\qquad\qquad \times\left(7\cdot 2^{2\,n}-126\cdot 2^n+584\right)\\
&4.\ M_f^{(16)} \geq -\frac{2^n\,(2^n-1)\,(2^n-2)\,(2^n-4)}{4515840}\\
&\qquad\qquad \times\left(24836\cdot 2^n-2275\cdot 2^{2n}+80\cdot 2^{3n}-92368\right)
\end{aligned}$$

Proof. 1. The codewords of $\mathcal{RM}(n-3,n)$ of Hamming weight 8 correspond to 3-dimensional flats of $\mathbb{F}_2^n$ that is

$$M_f^{(8)} = \sum_{A\in\mathcal{A}_3}(-1)^{\sum_{x\in A} f(x)}$$

Every 3-dimensional flat is, in $2(2^3-1)$ ways, the union of two distinct parallel 2-dimensional flats. Indeed, we know that there are $2(2^3-1)$ affine hyperplanes in any 3-dimensional flat. Hence

$$\begin{aligned}
&\sum_{A\in\mathcal{A}_3}(-1)^{\sum_{x\in A} f(x)} = \frac{1}{2(2^3-1)}\\
&\times\left(\sum_{\substack{(A,A')\in\mathcal{A}_2\times\mathcal{A}_2\\ A\parallel A'}}(-1)^{\sum_{x\in A} f(x)+\sum_{x\in A'} f(x)} - \#\mathcal{A}_2\right)
\end{aligned}$$

where $A \parallel A'$ means that A and A' have the same direction and are not necessarily distinct. Every $A\in\mathcal{A}_2$ can be written in 2^2 ways in the form $a+E$, where $a\in\mathbb{F}_2^n$ and $E\in\mathcal{E}_2$. We deduce that the sum $\sum_{A\in\mathcal{A}_3}(-1)^{\sum_{x\in A} f(x)}$ times $2(2^3-1)$ equals

$$\begin{aligned}
&\frac{1}{2^4}\sum_{E\in\mathcal{E}_2}\sum_{a,a'\in\mathbb{F}_2^n}(-1)^{\sum_{x\in a+E} f(x)+\sum_{x\in a'+E} f(x)} - \#\mathcal{A}_2\\
&=\frac{1}{2^4}\sum_{E\in\mathcal{E}_2}\left(\sum_{a\in\mathbb{F}_2^n}(-1)^{\sum_{x\in a+E} f(x)}\right)^2 - \#\mathcal{A}_2
\end{aligned}$$

from which we deduce that $\sum_{A\in\mathcal{A}_3}(-1)^{\sum_{x\in A} f(x)} \geq -\frac{\#\mathcal{A}_2}{2(2^3-1)}$ which proves the result since the size of $\mathcal{A}_2$ is equal to $2^{n-2}\prod_{i=0}^{1}\frac{2^n-2^i}{2^2-2^i}$.

2. According to the uniqueness of the representation of those codewords of weight 12 in the Reed-Muller code $\mathcal{RM}(n-3,n)$ as the indicators of those sets of the form $(A_1\cup A_2)\backslash(A_1\cap A_2)$, the character sum $M_f^{(12)}$ can be written as

$$M_f^{(12)} = \frac{1}{2}\sum_{\substack{A_1,A_2\in\mathcal{A}_3\\ \dim(A_1\cap A_2)=1}}(-1)^{\sum_{x\in A_1} f(x)+\sum_{x\in A_2} f(x)}$$

Therefore, denoting by $\mathcal{E}'_2$ the set of those 2-dimensional vector subspaces of an $(n-1)$-dimensional space over $\mathbb{F}_2$, $M_f^{(12)}$ can be rewritten as

$$\frac{1}{2}\sum_{A\in\mathcal{A}_1}\sum_{\substack{(E,E')\in\mathcal{E}'_2\times\mathcal{E}'_2\\ E\cap E'=\{0\}}}(-1)^{\sum_{x\in A+E}f(x)+\sum_{x\in A+E'}f(x)}$$

We make here an abuse of notation: E and E' should be two vector subspaces of a given $(n-1)$-dimensional space in a direct sum with the direction of A. We then deduce that $M_f^{(12)}$ is greater than or equal to

$$\geq \frac{1}{2}\sum_{A\in\mathcal{A}_1}\left(\sum_{(E,E')\in\mathcal{E}'_2\times\mathcal{E}'_2}(-1)^{\sum_{x\in A+E}f(x)+\sum_{x\in A+E'}f(x)}\right.$$
$$\left.-\#\mathcal{E}'_2-(2^{n-1}-1)(2^{n-2}-1)(2^{n-2}-2)\right).$$

The term "$-\#\mathcal{E}'_2$" above corresponds to the number of cases where $E=E'$ while the term "$-(2^{n-1}-1)(2^{n-2}-1)(2^{n-2}-2)$" is derived from the inequality

$$(-1)^{\sum_{x\in A+E}f(x)+\sum_{x\in A+E'}f(x)}\leq 1$$

when $E\cap E'$ is a 1-dimensional space. Noting that

$$\sum_{A\in\mathcal{A}_1}\sum_{(E,E')\in\mathcal{E}'_2\times\mathcal{E}'_2}(-1)^{\sum_{x\in A+E}f(x)+\sum_{x\in A+E'}f(x)}$$
$$=\sum_{A\in\mathcal{A}_1}\left(\sum_{E\in\mathcal{E}'_2}(-1)^{\sum_{x\in A+E}f(x)}\right)^2$$

and recalling that $\#\mathcal{E}'_2=\frac{(2^{n-1}-1)(2^{n-1}-2)}{(2^2-1)(2^2-2)}$ leads to the result.

3. According to the uniqueness of the representation of those codewords of Hamming weight 14, we have $M_f^{(14)}=\frac{1}{2}\sum_{u\in\mathbb{F}_2^n}\sum_{\substack{(E_1,E_2)\in\mathcal{E}_3\times\mathcal{E}_3\\ E_1\cap E_2=\{0\}}}(-1)^{\sum_{x\in u+E_1}f(x)+\sum_{x\in u+E_2}f(x)}$ and therefore

$$M_f^{(14)}\geq\frac{1}{2}\sum_{u\in\mathbb{F}_2^n}\left(\left(\sum_{E\in\mathcal{E}_3}(-1)^{\sum_{x\in u+E}f(x)}\right)^2\right.$$
$$-\frac{(2^n-1)(2^n-2)(2^n-4)}{(2^3-1)(2^3-2)(2^3-4)}$$
$$-\frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}(2^{n-2}-1)(2^{n-2}-2)$$
$$-(2^n-1)\cdot\frac{(2^{n-1}-1)(2^{n-1}-2)}{(2^2-1)(2^2-2)}$$
$$\left.\cdot\frac{(2^{n-1}-4)(2^{n-1}-8)}{(2^2-1)(2^2-2)}\right)$$

The term "$-\frac{(2^n-1)(2^n-2)(2^n-4)}{(2^3-1)(2^3-2)(2^3-4)}$" corresponds to the case where the vector subspaces E_1 and E_2 are equal. The others term "$-\frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}(2^{n-2}-1)(2^{n-2}-2)$" and "$-(2^n-1)\cdot\frac{(2^{n-1}-1)(2^{n-1}-2)}{(2^2-1)(2^2-2)}\cdot\frac{(2^{n-1}-4)(2^{n-1}-8)}{(2^2-1)(2^2-2)}$" are derived from the inequality

$$(-1)^{\sum_{x\in u+E_1} f(x)+\sum_{x\in u+E_2} f(x)} \leq 1$$

when $E_1 \cap E_2$ is, respectively, a 2-dimensional space and a 1-dimensional space.

4. The codewords of weight 16 are the sums of two codewords of minimal weight and having non-intersecting supports, i.e. are the indicators of those sets of the form $U = A_1 \cup A_2$ where A_1 and A_2 are two non-intersecting 3-dimensional flats. Some of them have more than one representation as sum of two codewords of minimal weight. According to [268], those codewords of Hamming weight 16 in the Reed-Muller code $\mathcal{RM}(n-3,n)$, which have more than one representation enter in two cases only:

   a. U is a 4-dimensional flat. The number of such codewords is obviously equal to $\frac{(2^n-1)(2^n-2)(2^n-4)(2^n-8)}{(2^4-1)(2^4-2)(2^4-4)(2^4-8)}$. And U is, in $2(2^4-1)$ ways, the union of an ordered pair of non-intersecting 3-dimensional parallel flats.

   b. U is the union of four distinct cosets of a 2-dimensional vector subspace, but is not a 4-dimensional flat. In this case, it is, in 3 ways, the union of two non-intersecting 3-dimensional flats. The number of such codewords equals $\frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}\cdot\left(\binom{2^{n-2}}{4}-\frac{1}{4}\binom{2^{n-2}}{3}\right)=\frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}\cdot\frac{2^{n-2}-4}{4}\cdot\binom{2^{n-2}}{3}$.

Therefore

$$\begin{aligned}
&\sum_{\substack{(A_1,A_2)\in\mathcal{A}_3^2\\ A_1\cap A_2=\emptyset}} (-1)^{\sum_{x\in A_1} f(x)+\sum_{x\in A_2} f(x)}\\
&= 2\cdot(2^4-1)\cdot \sum_{\substack{g\in\mathcal{RM}(n-3,n)\\ \mathrm{wt}(g)=16\\ g \text{ is of type a}}} (-1)^{\langle f,g\rangle}\\
&\quad +2\cdot 3\cdot \sum_{\substack{g\in\mathcal{RM}(n-3,n)\\ \mathrm{wt}(g)=16\\ g \text{ is of type b}}} (-1)^{\langle f,g\rangle}\\
&\quad +2\cdot \sum_{\substack{g\in\mathcal{RM}(n-3,n)\\ \mathrm{wt}(g)=16\\ g \text{ is neither of type a nor of type b}}} (-1)^{\langle f,g\rangle}\\
&= 2\cdot M_f^{(16)}\\
&\quad +2\cdot((2^4-1)-1)\cdot \sum_{\substack{g\in\mathcal{RM}(n-3,n)\\ \mathrm{wt}(g)=16\\ g \text{ is of type a}}} (-1)^{\langle f,g\rangle}\\
&\quad +2\cdot(3-1)\cdot \sum_{\substack{g\in\mathcal{RM}(n-3,n)\\ \mathrm{wt}(g)=16\\ g \text{ is of type b}}} (-1)^{\langle f,g\rangle}
\end{aligned}$$

Thus

$$\begin{aligned}
M_f^{(16)} &\geq \frac{1}{2} \sum_{\substack{(A_1,A_2)\in\mathcal{A}_3^2 \\ A_1\cap A_2=\emptyset}} (-1)^{\sum_{x\in A_1} f(x)+\sum_{x\in A_2} f(x)} \\
&\quad -(2^4-2)\cdot 2^{n-4}\prod_{j=0}^{3}\frac{2^n-2^j}{2^4-2^j} \\
&\quad -(3-1)\cdot(2^{n-4}-1)\cdot\binom{2^{n-2}}{3} \\
&\quad \cdot\frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)} \\
&\geq \frac{1}{2}\left(\sum_{A\in\mathcal{A}_3}(-1)^{\sum_{x\in A} f(x)}\right)^2 \\
&\quad -\frac{1}{2}\sum_{\substack{(A_1,A_2)\in\mathcal{A}_3^2 \\ A_1\cap A_2\neq\emptyset}} (-1)^{\sum_{x\in A_1\cup A_2} f(x)} \\
&\quad -14\cdot 2^{n-4}\prod_{j=0}^{3}\frac{2^n-2^j}{2^4-2^j} \\
&\quad -2\cdot(2^{n-4}-1)\cdot\binom{2^{n-2}}{3} \\
&\quad \cdot\frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}
\end{aligned}$$

We need now to evaluate the sum $\sum_{\{A_1,A_2\}\in\mathcal{A}_3\,|A_1\cap A_2\neq\emptyset} (-1)^{\sum_{x\in A_1\cup A_2} f(x)}$. Two 3-dimensional flats A_1 and A_2 which are not disjoint are necessarily of the form $A_1 = u+E_1$ and $A_2 = u+E_2$ where $u \in F_2^n$ and where E_1 and E_2 are two 3-dimensional spaces of F_2^n. There are 2^p ways

of choosing u if $\dim(E_1 \cap E_2) = p$.

$$\begin{aligned}
M_f^{(16)} \geq -\frac{1}{2}\Bigg(& 2^{n-2} \times \frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)} \\
& \times (2^{n-2}-1)(2^{n-2}-2) + 2^{n-1} \cdot (2^n-1) \\
& \times \frac{(2^{n-1}-1)(2^{n-1}-2)}{(2^2-1)(2^2-2)} \\
& \quad \times \frac{(2^{n-1}-4)(2^{n-1}-8)}{(2^2-1)(2^2-2)} \\
& + 2^n \times \frac{(2^n-1)(2^n-2)(2^n-4)}{(2^3-1)(2^3-2)(2^3-4)} \\
& \times \frac{(2^n-8)(2^n-16)(2^n-32)}{(2^3-1)(2^3-2)(2^3-4)} + 2^{n-3} \\
& \times \frac{(2^n-1)(2^n-2)(2^n-4)}{(2^3-1)(2^3-2)(2^3-4)} \Bigg) \\
& - 14 \cdot 2^{n-4} \prod_{j=0}^{3} \frac{2^n - 2^j}{2^4 - 2^j} \\
& - 2 \cdot (2^{n-4}-1) \cdot \binom{2^{n-2}}{3} \cdot \frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)}
\end{aligned}$$

The term "$\frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)} \cdot (2^{n-2}-1)(2^{n-2}-2)$" corresponds to the case where $E_1 \cap E_2$ is a 2-dimensional space, the term "$(2^n-1) \cdot \frac{(2^{n-1}-1)(2^{n-1}-2)}{(2^2-1)(2^2-2)} \cdot \frac{(2^{n-1}-4)(2^{n-1}-8)}{(2^2-1)(2^2-2)}$" to the case where $E_1 \cap E_2$ is a 1-dimensional space and the term "$\frac{(2^n-1)(2^n-2)(2^n-4)}{(2^3-1)(2^3-2)(2^3-4)} \cdot \frac{(2^n-8)(2^n-16)(2^n-32)}{(2^3-1)(2^3-2)(2^3-4)}$" to the case where the intersection $E_1 \cap E_2$ is trivial while the term "$2^{n-3} \cdot \frac{(2^n-1)(2^n-2)(2^n-4)}{(2^3-1)(2^3-2)(2^3-4)}$" is the cardinality of $\mathcal{A}_3$.

□

9.2.4 Upper bounds on $\rho(2, n)$

We first state a technical result which shall help us in establishing our upper bounds on the covering radius

Lemma 9.2.11. *([43]) Let A and B be two affine maps from $\mathbb{R}^n$ to $\mathbb{R}$. Let F be the multivariate fraction defined as $F(x) = \frac{A(x)}{B(x)}$. Let $y \in \mathbb{R}^n$ and set $\mathcal{D}_y = \{x \in \mathbb{R}^n \mid x_i \geq y_i, 1 \leq i \leq n\}$. Assume that $B(x) > 0$ for all $x \in \mathcal{D}_y$ and that, for all $1 \leq i \leq n$, $\frac{\partial F}{\partial x_i}(y) \geq 0$. Then, $\forall x \in \mathcal{D}_y$, $F(x) \geq F(y)$.*

Proof. Assume that the expressions of A and B are : $A(x) = a_0 + \sum_{i=1}^n a_i x_i$ and $B(x) = b_0 + \sum_{i=1}^n b_i x_i$. Straightforward calculations show that

$$F(x) - F(y) = \frac{\sum_{i=1}^n (a_i B(y) - b_i A(y))(x_i - y_i)}{B(x)B(y)}$$

Now $\frac{\partial F}{\partial x_i}(y) = \frac{a_i B(y) - b_i A(y)}{B^2(y)}$. The hypothesis on $\frac{\partial F}{\partial x_i}(y)$ implies that $a_i B(y) - b_i A(y) \geq 0$ for $1 \leq i \leq n$. Moreover, for all $x \in \mathcal{D}_y$, $B(x) > 0$. Hence $F(x) - F(y) \geq 0$ whenever $x \in \mathcal{D}_y$. □

We shall use Lemma 9.2.11 to establish our upper bounds on $\rho(2,n)$. Our approach is to consider the quotient $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}$ as a multivariate fraction in $M_f^{(8)}$, $M_f^{(12)}$, $M_f^{(14)}$ and $M_f^{(16)}$. Proposition 9.2.10 provides lower bounds on the character sums $M_f^{(2w)}$ for $2w = 8$, 12, 14 and 16 which we denote by $M_{min}^{(2w)}$ from now on. Set $\mathcal{D} = \{(X_8, X_{12}, X_{14}, X_{16}) \in \mathbb{R}^4 \mid X_{2w} \geq M_{min}^{(2w)},\ 2w = 8, 12, 14, 16\}$ and

$$
\begin{aligned}
F_3(X_8, X_{12}, X_{14}, X_{16}) &= \frac{D_4 + N_4^{(8)} X_8}{D_3} \\
F_4(X_8, X_{12}, X_{14}, X_{16}) &= \frac{D_5 + N_5^{(8)} X_8}{D_4 + N_4^{(8)} X_8} \\
F_5(X_8, X_{12}, X_{14}, X_{16}) &= \frac{D_6 + N_6^{(8)} X_8 + N_6^{(12)} X_{12}}{D_5 + N_5^{(8)} X_8} \\
F_6(X_8, X_{12}, X_{14}, X_{16}) & \\
&= \frac{D_7 + N_7^{(8)} X_8 + N_7^{(12)} X_{12} + N_7^{(14)} X_{14}}{D_6 + N_6^{(8)} X_8 + N_6^{(12)} X_{12}} \\
F_7(X_8, X_{12}, X_{14}, X_{16}) & \\
&= \frac{D_8 + N_8^{(8)} X_8 + N_8^{(12)} X_{12} + N_8^{(14)} X_{14} + N_8^{(16)} X_{16}}{D_7 + N_7^{(8)} X_8 + N_7^{(12)} X_{12} + N_7^{(14)} X_{14}}
\end{aligned}
$$

so that $\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} = F_k(M_f^{(8)}, M_f^{(12)}, M_f^{(14)}, M_f^{(16)})$, $k \in \{3,4,5,6,7\}$. Moreover, we denote by B_{k+1} (resp. B_k) the numerator (resp. the denominator) of F_k : $F_k = \frac{B_{k+1}}{B_k}$. In order to apply Lemma 9.2.11, we first have to check that B_k, $3 \leq k \leq 7$, is non-negative on $\mathcal{D}$ which is equivalent to check that $B_k(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)})$ is non-negative; using Lemma 9.2.7 and Proposition 9.2.10, we compute the expressions of $B_k(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)})$:

$$B_3(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)}) = 16 \cdot 2^n - 30 \cdot 2^{2n} + 15 \cdot 2^{3n}$$

$$B_4(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)}) = 948 \cdot 2^{2n} - 512 \cdot 2^n - 540 \cdot 2^{3n} + 105 \cdot 2^{4n}$$

$$B_5(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)}) = 65536 \cdot 2^n - 116160 \cdot 2^{2n} + 61380 \cdot 2^{3n} - 11700 \cdot 2^{4n} + 945 \cdot 2^{5n}$$

$$B_6(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)}) = 402027648 \cdot 2^{2n} - 211849472 \cdot 2^n - 240291480 \cdot 2^{3n} + 54127260 \cdot 2^{4n} - 4024350 \cdot 2^{5n} + 10395 \cdot 2^{6n}$$

$$B_7(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)}) = 198419424256 \cdot 2^n - 398672851200 \cdot 2^{2n} + 267026348160 \cdot 2^{3n} - 75744669000 \cdot 2^{4n} + 9395125740 \cdot 2^{5n} - 423513090 \cdot 2^{6n} + 135135 \cdot 2^{7n}$$

$$B_8(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)}) = 291614802947328 \cdot 2^{2n} - 138500717330432 \cdot 2^n - 213269835467520 \cdot 2^{3n} + 70986429811440 \cdot 2^{4n} - 11750204466000 \cdot 2^{5n} + 949606617960 \cdot 2^{6n} - 30084139800 \cdot 2^{7n} + 2027025 \cdot 2^{8n}$$

All of these expressions are polynomials in 2^n and can be negative for small values of n. Now, given a polynomial $p(x) = \sum_{i=0}^{d} a_i x^i$ whose leading coefficient a_d is positive, one can show that $p(x)$ is positive whenever x is an integer greater than $\sum_{i=0}^{d-1} \frac{|a_i|}{a_d}$. In the particular case where $x = 2^n$, that corresponds to say that $p(2^n)$ is positive as soon as $n \geq \left\lceil \log_2 \left(\sum_{i=0}^{d-1} \frac{|a_i|}{a_d} \right) \right\rceil$. For the other values of n, we can check by computer calculations whether $p(2^n)$ is positive or

k	3	4	5	6	7	8
N_k	1	1	1	9	12	14

Table 9.3 – Values of N_k for $k \leq 8$

k	3	4	5	6	7
N'_k	1	3	1	4	11

Table 9.4 – Values of N_k for $k \leq 7$

not. For each value of k in $\{3,4,5,6,7,8\}$, we compute with this method the smallest positive integer N_k such that $B_k(M^{(8)}_{min}, M^{(12)}_{min}, M^{(14)}_{min}, M^{(16)}_{min})$ is non-negative for all $n \geq N_k$ (Table 9.3). Next, we have to check that all the derivatives of each multivariate fraction F_k evaluated at $(M^{(8)}_{min}, M^{(12)}_{min}, M^{(14)}_{min}, M^{(16)}_{min})$ are non-negative. We only have to check that the numerator $R_{k,2w}$ of $\frac{\partial F_k}{\partial X_{2w}}(M^{(8)}_{min}, M^{(12)}_{min}, M^{(14)}_{min}, M^{(16)}_{min})$ is non-negative. We present below all these derivatives :
$R_{3,8} = 40320, \quad R_{3,12} = R_{3,14} = R_{3,16} = 0$

$R_{4,8} = 2312110080 \cdot 2^n - 5419008000 \cdot 2^{2n} + 4470681600 \cdot 2^{3n} - 1524096000 \cdot 2^{4n} + 152409600 \cdot 2^{5n}, \quad R_{4,12} = R_{4,14} = R_{4,16} = 0$

$R_{5,8} = 3997794034483200 \cdot 2^{2n} - 1918876802088960 \cdot 2^n - 2849111735500800 \cdot 2^{3n} + 887743245312000 \cdot 2^{4n} - 123645641011200 \cdot 2^{5n} + 6060567744000 \cdot 2^{6n} + 37721376000 \cdot 2^{7n}, \quad R_{5,12} = 479001600, \quad R_{5,14} = R_{5,16} = 0$

$R_{6,8} = 714305067842528870400 \cdot 2^{2n} - 304823802557670359040 \cdot 2^n - 623442323326323916800 \cdot 2^{3n} + 270672649382777241600 \cdot 2^{4n} - 64840249978798694400 \cdot 2^{5n} + 8729057509549977600 \cdot 2^{6n} - 618210641983334400 \cdot 2^{7n} + 17800717334400000 \cdot 2^{8n} + 10788313536000 \cdot 2^{9n}$

$R_{6,12} = 41538262649890406400 \cdot 2^{2n} - 21168521847373824000 \cdot 2^n - 26589203861623603200 \cdot 2^{3n} + 6932829197758464000 \cdot 2^{4n} - 737575419829248000 \cdot 2^{5n} + 23820596287488000 \cdot 2^{6n} + 388379287296000 \cdot 2^{7n}, \quad R_{6,14} = 87178291200, \quad R_{6,16} = 0$

$R_{7,8} = 10108016046304557677936640 0 \cdot 2^{2n} - 39412011145610093490339840 \cdot 2^n - 10161505165286281016770560 0 \cdot 2^{3n} + 54155713559386060932710400 \cdot 2^{4n} - 17273494380961564294348800 \cdot 2^{5n} + 3477651223865798717337600 \cdot 2^{6n} - 4470501693707748002304 00 \cdot 2^{7n} + 3566093998553678592000 0 \cdot 2^{8n} - 161028437036872204800 0 \cdot 2^{9n} + 31443268011835680000 \cdot 2^{10n} + 3681511994160000 \cdot 2^{11n}$

$R_{7,12} = 24562070787228570589593600 \cdot 2^{2n} - 11210398018269596142796800 \cdot 2^n - 19274531256693766442188800 \cdot 2^{3n} + 72105781026030249738240 00 \cdot 2^{4n} - 14356310231149470904320 00 \cdot 2^{5n} + 1565385340108480450560 00 \cdot 2^{6n} - 882591464325015244800 0 \cdot 2^{7n} + 198523956494223360000 \cdot 2^{8n} + 265068863579520000 \cdot 2^{9n}$

$R_{7,14} = 1557955581743194448855040 0 \cdot 2^{2n} - 7299354442387733191065600 \cdot 2^n - 1165054315581106952601600 0 \cdot 2^{3n} + 4000678147446896627712000 \cdot 2^{4n} - 685369279252080783360000 \cdot 2^{5n} + 568527238341918535680000 \cdot 2^{6n} - 182104833744497664000 0 \cdot 2^{7n} + 1236988030037760000 \cdot 2^{8n}$

$R_{7,16} = 20922789888000$

All these expressions are polynomials in 2^n and can be negative for small values of n. Therefore, for each value of k in $\{3,4,5,6,7\}$, we compute the smallest positive integer N'_k such that $\min(R_{k,8}, R_{k,12}, R_{k,14}, R_{k,16})$ is non-negative for all $n \geq N'_k$ (Table 9.4). The method used is the same one as that used for Table 9.3. Given $k \in \{3,4,5,6,7\}$, the mapping F_k satisfies all the conditions of Lemma 9.2.11 provided that n is greater than or equal to $\max(N_k, N'_k)$. Hence,

we have, for every $k \in \{3,4,5,6,7\}$,

$$\min_{f\in\mathcal{B}_n} \frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)} \geq \frac{B_{k+1}(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)})}{B_k(M_{min}^{(8)}, M_{min}^{(12)}, M_{min}^{(14)}, M_{min}^{(16)})} \tag{9.13}$$

We now present the upper bounds on $\rho(2,n)$ which we deduce from (9.13) and the restrictions on the values of k.

1. For $n \in \{3,4,5,6,7,8\}$: One can only consider the values of $k \leq 4$ in (9.13), since according to the first tabular, we must have $k+1 \leq 5$. This gives, for instance, $\rho(2,3) \leq 1$, $\rho(2,4) \leq 3$, $\rho(2,5) \leq 8$, $\rho(2,6) \leq 20$, $\rho(2,7) \leq 47$ and $\rho(2,8) \leq 104$. None of these values improves upon the known bounds on $\rho(2,n)$ for $n = 6$, 7, 8 which are presented in table 9.1.

2. For $n \in \{9,10,11\}$: We can consider $k = 5$ in addition to $k \leq 4$ for $n \in \{9,10,11\}$. This gives $\rho(2,9) \leq 222$, $\rho(2,10) \leq 464$, $\rho(2,11) \leq 956$. The upper bound on $\rho(2,9)$ is still worse than the one presented in table 9.1. Our bound begins to improve upon the known bounds for $n \geq 10$ (i.e. the results that we can deduce from the upper bound on $\rho(1,n)$ and from the recursive inequality (9.3)).

3. For $n \in \{12,13\}$: considering $k = 6$, we get $\rho(2,12) \leq 1946$ and $\rho(2,13) \leq 3949$, which are better than the known results.

4. For $n \geq 14$: All the values of k can be taken in (9.13). We have checked that the best upper bound is given by taking $k = 7$ only if $n \geq 17$ while for $n = 14$, 15, 16, the best upper bounds are obtained with smaller values of k : $\rho(2,14) \leq 7981$, $\rho(2,15) \leq 16071$ and $\rho(2,16) \leq 32316$. For $n \geq 17$, we obtain the following upper bound :

$$\rho(2,n) \leq \left\lfloor 2^{n-1} - \frac{1}{2}\sqrt{\frac{A_n}{B_n}} \right\rfloor$$

with

$$\begin{aligned} A_n = {} & 291614802947328 \cdot 2^{2n} - 138500717330432 \cdot 2^n \\ & - 213269835467520 \cdot 2^{3n} + 70986429811440 \cdot 2^{4n} \\ & - 11750204466000 \cdot 2^{5n} + 949606617960 \cdot 2^{6n} \\ & - 30084139800 \cdot 2^{7n} + 2027025 \cdot 2^{8n} \end{aligned}$$

$$\begin{aligned} B_n = {} & 198419424256 \cdot 2^n - 398672851200 \cdot 2^{2n} \\ & + 267026348160 \cdot 2^{3n} - 75744669000 \cdot 2^{4n} \\ & + 9395125740 \cdot 2^{5n} - 423513090 \cdot 2^{6n} \\ & + 135135 \cdot 2^{7n} \end{aligned}$$

In order to simplify our upper bound on $\rho(2,n)$, we compute a series expansion of $\sqrt{\frac{A_n}{B_n}}$ as n tends to infinity,

$$\begin{aligned} \sqrt{\frac{A_n}{B_n}} = \sqrt{15}\Bigg(& 2^{\frac{n}{2}} - \frac{122929}{21} \cdot 2^{-\frac{n}{2}} \\ & - \frac{155582504573}{4410} \cdot 2^{-\frac{3n}{2}} + O\left(2^{-\frac{5n}{2}}\right) \Bigg) \end{aligned}$$

By controlling the remainder more precisely, we can proved that, for every $n \geq 17$, the integer part of the two sides of the latter equation are equal (the proof is tedious and omitted)

$$\left\lfloor 2^{n-1} - \frac{1}{2}\sqrt{\frac{A_n}{B_n}} \right\rfloor = \left\lfloor 2^{n-1} - \frac{\sqrt{15}}{2}\, 2^{\frac{n}{2}} \left(1 - \frac{122929}{21 \cdot 2^n} - \frac{155582504573}{4410 \cdot 2^{2n}}\right)\right\rfloor$$

9.3 Final remarks

1. $\max_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)}\right)^2$ can then be lower bounded in several other ways, with the same principle by considering quotients like $\frac{\mathcal{S}_{k+p}(f)}{\mathcal{S}_k(f)}$ where p is a positive integer greater than 1. But computer calculations revealed that the best lower bound is actually obtained by letting $p = 1$.

2. As shown in [243, Table I, (5), (6) and p. 392, (c) $N_{m,r,2^{m-r+1}+2^{m-r-2}}$], the codewords of Hamming weight 18 in $RM(n-3,n)$ are either of the form $X_1X_2X_3 + X_4(X_2X_5 + X_3X_6 + X_7X_8 + X_9X_{10} + X_{11}X_{12})$ or of the form $X_1X_2X_3 + X_4(X_3X_5 + X_6X_7 + X_8X_9 + X_{10}X_{11} + X_{12}X_{13}$ (where X_1, X_2, ... are mutually independent polynomials). The number of these codewords is equal to $104811 \begin{bmatrix} n \\ 6 \end{bmatrix} 2^{n+8} + 26043255 \begin{bmatrix} n \\ 7 \end{bmatrix} 2^{n+12} + 77302995 \begin{bmatrix} n \\ 8 \end{bmatrix} 2^{n+20} + \begin{bmatrix} n \\ 5 \end{bmatrix} 2^{n-5} N_{5,2,18}$ where $N_{5,2,18}$ denotes the number of cubic Boolean functions of $\mathcal{RM}(2,5)$ of Hamming weight 18. Although the codewords of Hamming weight 18 as well as their number are known, we were not able to get any significant lower bounds on the character sums $M_f^{(18)}$.

3. The same method as in Theorem 9.1.1 could be applied to the Reed-Muller code of order r. Inequality (9.9) would conduce to an upper bound of the form $2^{n-1} - \sqrt{2k+1} \cdot 2^{\frac{n}{2}-1} + O(n^{r-2})$. Therefore, such an upper bound would improve upon Theorem 9.1.2 only if $\sqrt{2k+1} \geq \sqrt{15}\,(1+\sqrt{2})^{r-2}$ which requires $2k \geq 15\,\left(\sqrt{2}+1\right)^{2r-4} - 1$. The dual code of $\mathcal{RM}(r,n)$ is $\mathcal{RM}(n-r-1,n)$ whose minimum distance is $d_{min} = 2^{r+1}$. Kasami and *al* [145, 243] only pushed their characterizations to 2.5 times the minimum distance of the Reed-Muller codes that is $5 \cdot 2^r$. It can be easily checked that $15\,\left(\sqrt{2}+1\right)^{2r-4} - 1 > 5 \cdot 2^r$ for every $r \geq 3$ which means that the knowledge of the codewords of $\mathcal{RM}(n-r-1,n)$ has not yet been pushed far enough to be able to use the method described in this subsection for $r \geq 3$.

9.4 Conclusion

We were able to improve upon the best known upper bounds on the covering radii of Reed-Muller codes thanks to the characterization, due to Kasami and Tokura, of those elements of the Reed-Muller codes whose Hamming weights are smaller than twice and a half the minimum distance. It seems that knowing more about the elements of small weights in the Reed-Muller codes would not permit to improve further our bounds. New ideas seem necessary for that.

Bibliography

[1] Omran Ahmadi and Robert Granger. An efficient deterministic test for Kloosterman sum zeros. *CoRR*, abs/1104.3882, 2011. (Cited on pages 250, 251, and 252.)

[2] Jörg Arndt. *Matters Computational: Ideas, Algorithms, Source Code*. Springer, 2010. (Cited on pages 103 and 251.)

[3] J-M. Le Bars and A. Viola. Equivalence classes of Boolean functions for first-order correlation. In *IEEE Transactions on Information Theory, Vol 56, no. 3*, pages 1247–1261, 2010. (Cited on pages 5, 69, 71, and 332.)

[4] T. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions. In *IEEE Trans. Inform. Theory, vol. 52, no. 9*, pages 4160–4170, 2006. (Cited on page 279.)

[5] Elwyn Ralph Berlekamp, Victor Henry Rumsey, and Hannah Greenebaum Solomon. On the solution of algebraic equations over finite fields. *Information and Control*, 10:553–564, 1967. (Cited on page 231.)

[6] Ian Fraser Blake, Gadiel Seroussi, and Nigel Paul Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original. (Cited on pages 222, 223, and 224.)

[7] Y. Borissov, A. Braeken, S. Nikova, and B. Preneel. On the covering radii of binary Reed-Muller codes in the set of resilient Boolean functions. In *IEEE Transactions on Information Theory, Vol. 51, no. 3*, pages 1182–1189, 2005. (Cited on pages 31 and 356.)

[8] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). (Cited on pages 232, 235, and 244.)

[9] Robert Bradshaw, Craig Citro, and Dag Sverre Seljebotn. Cython: the best of both worlds. *CiSE 2011 Special Python Issue*, page 25, 2010. (Cited on pages 21, 168, and 346.)

[10] Richard Peirce Brent, Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann. Faster multiplication in GF(2)[x]. In Alfred Jacobus van der Poorten and Andreas Stein, editors, *ANTS*, volume 5011 of *Lecture Notes in Computer Science*, pages 153–166. Springer, 2008. (Cited on pages 21, 168, and 346.)

[11] Julia M.N. Brown and William E. Cherowitzo. The Lunelli-Sce hyperoval in $PG(2, 16)$. In *J. Geom. (69), no. 1-2*, pages 15–36, 2000. (Cited on page 148.)

[12] L. Budaghyan and C. Carlet. On CCZ-equivalence and its use in secondary constructions of bent functions. In *Proceedings of the International Workshop on Coding and Cryptography WCC 2009.* (Cited on pages 18, 117, and 344.)

[13] L. Budaghyan and C. Carlet. CCZ-equivalence of single and multi output Boolean functions. In *AMS Contemporary Math. 518, Post-proceedings of the conference Fq 9*, pages 43–54, 2010. (Cited on page 18.)

[14] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager. Further results on Niho bent functions. In *IEEE Transactions on Information Theory-IT, Vol 58, no.11*, pages 6979–6985, 2012. (Cited on pages 19, 133, 135, 136, and 345.)

[15] H. Dobbertin C. Carlet and G. Leander. Normal extensions of bent functions. In *EEE Transactions on Information Theory, vol. 50, no. 11*, pages 2880–2885, 2004. (Cited on page 111.)

[16] C. Carlet and S. Mesnager. On the construction of bent vectorial functions. In *Journal of Information and Coding Theory: Algebraic and Combinatorial Coding Theory Vol 1, no. 2*, pages 133–148, 2010. (Cited on pages 19, 116, 117, 118, 119, 120, 121, and 344.)

[17] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Crypto'91, Advance in Cryptology, Lecture Notes in Computer Science 576*, pages 86–100, 1991. (Cited on pages 5, 69, 70, and 332.)

[18] E. Rodney Canfield, Zhicheng Gao, Catherine Greenhill, Brendan D. McKay, and Robert W. Robinson. Asymptotic enumeration of correlation-immune boolean functions. In *Journal of Cryptography and Communications, Vol 2, no. 1*, pages 111–126, 2010. (Cited on pages 5, 78, and 332.)

[19] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of R(1,m). In *IEEE Transactions on Information Theory, vol. 47*, pages 1494–1513, 2001. (Cited on pages 27, 255, 351, and 352.)

[20] A. Canteaut and P. Charpin. Decomposing bent functions. In *IEEE Transactions on Information Theory, Vol 49*, pages 2004–2019, 2003. (Cited on pages 27 and 352.)

[21] A. Canteaut, P. Charpin, and G. Kyureghyan. A New Class of Monomial Bent Functions. In *Finite Fields and Their Applications, Vol 14, no. 1*, pages 221–241, 2008. (Cited on page 107.)

[22] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In *Advanced in Cryptology-EUROCRYPT 2000. Lecture notes in computer science, 1807*, pages 573–588, 2000. (Cited on pages 2, 4, 60, 63, 64, 330, and 331.)

[23] C. Carlet. Vectorial Boolean Functions for Cryptography. In *Chapter of the monography Boolean Methods and Models, Y. Crama and P. Hammer eds, Cambridge University Press. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html.* (Cited on page 115.)

[24] C. Carlet. Two new classes of bent functions. In *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 77–101, 1994. (Cited on pages 110, 121, 126, and 278.)

[25] C. Carlet. Generalized partial spreads. In *IEEE Trans. Inform. Theory, vol. 41, no. 5*, pages 1482–1487, 1995. (Cited on page 278.)

[26] C. Carlet. A construction of bent functions. In *Finite Fields and Applications, London Mathematical Society, Lecture Series 233, Cambridge University Press*, pages 47–58, 1996. (Cited on pages 110, 111, and 115.)

[27] C. Carlet. On the confusion and diffusion properties of Maiorana-McFarland's and extended Maiorana-McFarland's functions. In *Complexity Issues in Coding and Cryptography, Special Issue dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity 20*, pages 182–204, 2004. (Cited on page 117.)

[28] C. Carlet. On the secondary constructions of resilient and bent functions. In *Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, published by Birkhäuser Verlag*, pages 3–28, 2004. (Cited on pages 111 and 118.)

[29] C. Carlet. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. In *AAECC 16, Las Vegas, february 2006, volume 3857 of Lecture Notes in Computer Science, Springer*, pages 1–28, 2006. (Cited on pages 68, 69, and 111.)

[30] C. Carlet. On the higher order nonlinearities of algebraic immune Boolean functions. In *CRYPTO 2006, ser. Lecture notes in Computer Science, vol. 4117*, pages 584–601, 2006. (Cited on pages xv, 6, 7, 8, 79, 80, 81, 84, 85, 86, 87, and 333.)

[31] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. In *Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.)*, pages 257–397, 2010. (Cited on pages 2, 11, 12, 27, 38, 39, 59, 60, 62, 66, 70, 103, 110, 111, 115, 116, 119, 123, 130, 132, 135, 137, 256, 330, 337, and 352.)

[32] C. Carlet. Relating three nonlinearity characteristics of vectorial functions and using bent functions to build APN and differentially 4-uniform functions. In *Des. Codes Cryptography, 59 (1–3)*, pages 89–109, 2011. (Cited on pages 18, 117, and 338.)

[33] C. Carlet, P. Charpin, , and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. In *Designs, Codes and Cryptography, 15(2), pp. 125-156*, 1998. (Cited on pages 18 and 344.)

[34] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra. Algebraic immunity for cryptographically significant boolean functions: Analysis and construction. In *IEEE Transactions on Information Theory, vol 52, no. 7*, pages 3105–3121, 2006. (Cited on pages xv, 7, 31, 79, 81, 84, 86, 87, 333, and 356.)

[35] C. Carlet, H. Dobbertin, and G. Leander. Normal extensions of bent functions. In *IEEE Trans. Inf. Theory, vol. 50, no. 11*, pages 2880–2885, 2004. (Cited on page 121.)

[36] C. Carlet and P. Gaborit. Hyperbent functions and cyclic codes. In *Journal of Combinatorial Theory, Series A, Vol 113, no. 3*, pages 466–482, 2006. (Cited on pages 151, 152, 153, and 154.)

[37] C. Carlet and A. Gouget. An upper bound on the number of m-resilient Boolean functions. In *ASIACRYPT 2002, Advances in Cryptology, Lecture Notes in Computer Science 2501*, pages 484–496, 2002. (Cited on pages 69, 71, and 332.)

[38] C. Carlet and P. Guillot. A new representation of Boolean functions. In *AAECC'13, Lecture Notes in Computer Science 1719*, pages 94–103, 1999. (Cited on pages 5, 38, and 332.)

[39] C. Carlet and P. Guillot. Bent, resilient Functions and the Numerical Normal Form. In *DIMACS, Discrete Mathematics and Theoretical Computer Science*, pages 87–96, 2001. (Cited on pages 5, 39, 70, and 332.)

[40] C. Carlet, P. Guillot, and S. Mesnager. On immunity profile of Boolean functions. In *Proceedings of SEquences and Their Applications, SETA 2006, Lecture Notes in Computer Science*, pages 364–375, 2006. (Cited on pages 10, 63, 66, 67, and 336.)

[41] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager. On the duals of bent functions with 2^r niho exponents. In *IEEE International Symposium on Information Theory, ISIT 2011*, pages 703–707, 2011. (Cited on pages 19, 109, 133, 135, 136, 138, and 345.)

[42] C. Carlet and A. Klapper. Upper bounds on the numbers of resilient functions and of bent functions. In *23rd Symposium on Information Theory in the Benelux, Louvain-La-Neuve, Belgique, Mays*, 2002. (Cited on pages 69, 71, and 332.)

[43] C. Carlet and S. Mesnager. Improving the upper bounds on the covering radii of binary Reed-Muller codes. In *IEEE Transactions on Information Theory, vol. 53, no. 1*, pages 162–173, 2007. (Cited on pages 31, 33, 287, 288, 289, 290, 292, 294, 296, 300, and 357.)

[44] C. Carlet and S. Mesnager. On Dillon's class H of bent functions, niho bent functions and O-polynomials. In *Journal of Combinatorial Theory, Series A, Vol 118, no. 8*, pages 2392–2410, 2011. (Cited on pages 19, 28, 109, 122, 123, 125, 127, 128, 130, 131, 132, 133, 135, 137, 140, 147, 148, 279, 344, and 353.)

[45] C. Carlet and S. Mesnager. On Semi-bent Boolean Functions. In *IEEE Transactions on Information Theory-IT, Vol 58 No 5*, pages 3287–3292, 2012. (Cited on pages 28, 30, 126, 276, 279, 280, 353, and 355.)

[46] C. Carlet and P. Sarkar. Spectral domain analysis of correlation immune and resilient boolean functions. In *Finite Fields and their Applications*, pages 120–130, 2002. (Cited on pages 3, 62, and 330.)

[47] Claude Carlet. On a weakness of the Tu-Deng function and its repair. Cryptology ePrint Archive, Report 2009/606, 2009. `http://eprint.iacr.org/`. (Cited on pages 9, 91, and 334.)

[48] Claude Carlet. Comments on "Constructions of cryptographically significant Boolean functions using primitive polynomials". *Information Theory, IEEE Transactions on*, 57(7):4852 –4853, july 2011. (Cited on page 88.)

[49] Claude Carlet, Deepak Kumar Dalai, Kishan Chand Gupta, and Subhamoy Maitra. Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction. *IEEE Transactions on Information Theory*, 52(7):3105–3121, 2006. (Cited on pages 8, 86, and 334.)

[50] Claude Carlet and Keqin Feng. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In Josef Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 425–440. Springer, 2008. (Cited on pages 9, 88, and 334.)

[51] Claude Carlet, Xiangyong Zeng, Chunlei Li, and Lei Hu. Further properties of several classes of Boolean functions with optimum algebraic immunity. *Des. Codes Cryptography*, 52(3):303–338, 2009. (Cited on pages 8, 86, and 334.)

[52] L. Carlitz. Explicit evualation of certain exponential sums. In *Math. Scand. Vol.44*, pages 5–16, 1979. (Cited on page 43.)

[53] F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. In *Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science 950*, pages 356–365, 1995. (Cited on pages 18 and 338.)

[54] P. Charpin and G. Gong. Hyperbent functions, Kloosterman sums and Dickson polynomials. In *IEEE Trans. Inform. Theory (54) 9*, pages 4230–4238, 2008. (Cited on pages 20, 21, 22, 23, 29, 106, 107, 153, 154, 155, 169, 180, 198, 280, 281, 345, 346, 348, 350, and 354.)

[55] P. Charpin and G. Gong. Hyperbent functions, Kloosterman sums and Dickson polynomials. In *ISIT 2008, Toronto, Canada, July 6–11*, pages 1758–1762, 2008. (Cited on pages 20 and 345.)

[56] P. Charpin, T. Helleseth, and V. Zinoviev. The divisibility modulo 24 of Kloosterman sums of $GF(2^m)$, m odd. *Journal of Combinatorial Theory, Series A*, 114:322–338, 2007. (Cited on pages 43, 45, 159, 175, and 262.)

[57] P. Charpin, T. Helleseth, and V. Zinoviev. Divisibility properties of Kloosterman sums over finite fields of characteristic two. In *ISIT 2008, Toronto, Canada, July 6 – 11*, pages 2608–2612, 2008. (Cited on pages 48, 52, 158, 162, 187, 188, and 191.)

[58] P. Charpin and G. Kyureghyan. Cubic monomial bent functions: A subclass of $\mathcal{M}$. In *SIAM, J. Discr. Math., Vol.22, no.2*, pages 650–665, 2008. (Cited on page 107.)

[59] P. Charpin, E. Pasalic, and C. Tavernier. On bent and semi-bent quadratic Boolean functions. In *IEEE Transactions on Information Theory, vol. 51, no. 12*, pages 4286–4298, 2005. (Cited on pages 27, 108, 255, and 352.)

[60] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Divisibility properties of Kloosterman sums over finite fields of characteristic two. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 2608 –2612, july 2008. (Cited on page 231.)

[61] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Divisibility properties of classical binary Kloosterman sums. *Discrete Mathematics*, 309(12):3975–3984, 2009. (Cited on pages 43, 53, and 249.)

[62] S. Chee, S. Lee, and K. Kim. Semi-bent Functions. In *Advances in Cryptology-ASIACRYPT94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, Wollongong, Australia. Pieprzyk, J. and Safavi-Naini, R., Eds., Lect. Notes Comp. Sci, vol 917*, pages 107–118, 1994. (Cited on pages 27, 255, 351, and 352.)

[63] J. H. Cheon and S. Chee. Elliptic curves and resilient functions. In *Lecture Notes in Computer Science, vol 2015*, pages 386–397, 2000. (Cited on pages 27 and 352.)

[64] V. Chepyzhov and B. Smeets. On a fast correlation attack on certain stream ciphers. In *Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science, 547*, pages 176–185, 1992. (Cited on page 60.)

[65] William E. Cherowitzo, Tim Penttila, Ivano Pinneri, and Gordon F. Royle. Flocks and ovals. In *Geom. Dedicata, 60, no. 1*, pages 17–37, 1996. (Cited on page 142.)

[66] Wun Seng Chou, Javier Gomez-Calderon, and Gary Lee Mullen. Value sets of Dickson polynomials over finite fields. *J. Number Theory*, 30(3):334–344, 1988. (Cited on pages 54 and 55.)

[67] G. Cohen and J-P. Flori. On a generalized combinatorial conjecture involving addition mod 2^k-1. Cryptology ePrint Archive, Report 2011/400, 2011. `http://eprint.iacr.org/`. (Cited on pages 10, 96, 99, and 336.)

[68] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. Covering codes. In *North Holland*, 1997. (Cited on pages 31, 104, 152, 285, 286, 291, and 355.)

[69] G. Cohen and S. Litsyn. On the covering radius of Reed-Muller codes. In *Discrete Mathematics, Vol. 106-107*, pages 147–155, 1992. (Cited on pages 31, 285, 286, and 355.)

[70] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. (Cited on pages 206 and 223.)

[71] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006. (Cited on page 224.)

[72] N. Courtois. Higher Order Correlation Attacks, XL algorithm, and Cryptanalysis of Toyocrypts. (Cited on pages 3, 6, 62, 79, 330, and 333.)

[73] N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *Eurocrypt 03, volume 2656 of Lecture Notes in Computer Science*, pages 345–349, 2003. (Cited on pages 3, 31, 62, 330, and 356.)

[74] Nicolas Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 176–194. Springer, 2003. (Cited on page 61.)

[75] Nicolas Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In Eli Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 345–359. Springer, 2003. (Cited on page 61.)

[76] David Archibald Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication. (Cited on page 223.)

[77] D. K. Dalai, K. C. Gupta, and S. Maitra. Notion of algebraic immunity and its evaluation related to fast algebraic attacks. In *International Workshop on Boolean Functions : Cryptography and Applications*, pages 13–15, 2006. (Cited on page 61.)

[78] Deepak Kumar Dalai, Subhamoy Maitra, and Sumanta Sarkar. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Des. Codes Cryptography*, 40(1):41–58, 2006. (Cited on pages 8, 86, and 334.)

[79] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. In Claus Fieker and David R. Kohel, editors, *ANTS*, volume 2369 of *Lecture Notes in Computer Science*, pages 308–323. Springer, 2002. (Cited on pages 224 and 235.)

[80] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *J. Cryptology*, 19(1):1–25, 2006. (Cited on page 224.)

[81] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941. (Cited on page 223.)

[82] J. Dillon. Elementary Hadamard difference sets. In *PhD dissertation, University of Maryland.* (Cited on pages 11, 12, 20, 88, 105, 106, 107, 110, 115, 154, 156, 276, 278, 279, 280, 336, 337, 338, and 345.)

[83] J. Dillon. A survey of bent functions. In *NSA Technical Journal Special Issue*, pages 191–215, 1972. (Cited on page 115.)

[84] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. In *Finite Fields and Their Applications Volume 10, Issue 3*, pages 342–389, 2004. (Cited on pages 45 and 107.)

[85] J. F. Dillon and G. McGuire. Near bent functions on a hyperplane. In *Finite Fields and Their Applications Vol. 14, Issue 3*, pages 715–720, 2008. (Cited on page 108.)

[86] John Francis Dillon. *Elementary Hadamard Difference Sets.* ProQuest LLC, Ann Arbor, MI, 1974. Thesis (Ph.D.)–University of Maryland, College Park. (Cited on pages 8, 88, and 334.)

[87] John Francis Dillon. *Elementary Hadamard Difference Sets.* PhD thesis, University of Maryland, 1974. (Cited on page 122.)

[88] John Francis Dillon and Hans Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004. (Cited on pages 53 and 231.)

[89] Cunsheng Ding, Guozhen Xiao, and Weijuan Shan. *The Stability Theory of Stream Ciphers*, volume 561 of *Lecture Notes in Computer Science.* Springer, 1991. (Cited on page 60.)

[90] H. Dobbertin. Proceedings of Fast Software Encryption, Second International Workshop. In *Lecture Notes in Computer Science 1008*, pages 61–74, 1995. (Cited on page 11.)

[91] H. Dobbertin. Uniformly representable permutation polynomials. In *Proceedings of Sequences and their Applications, SETA 01, Discrete Mathematics and Theoretical Computer Science, Springer*, pages 1–22, 2002. (Cited on pages 137 and 138.)

[92] H. Dobbertin and G. Leander. Cryptographer[U+FFFD] Toolkit for Construction of 8-Bit Bent Functions. In *Cryptology ePrint Archive, Report no. 2005/089. Available at http://eprint.iacr.org/2005/089*, 2005. (Cited on pages 27 and 351.)

[93] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit. Construction of bent functions via Niho Power Functions. In *Journal of Combinatorial therory, Serie A 113*, pages 779–798, 2006. (Cited on pages 13, 14, 15, 29, 108, 109, 125, 126, 132, 133, 138, 139, 141, 146, 258, 261, 280, 281, 338, 339, 340, 342, 343, 353, and 354.)

[94] Hans Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In Bart Preneel, editor, *FSE*, volume 1008 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1994. (Cited on pages 9, 90, and 334.)

[95] François G. Dorais and Dominic W. Klyve. A Wieferich prime search up to 6.7×10^{15}. *Journal of Integer Sequences*, 14(9), 2011. Available online at `http://www.cs.uwaterloo.ca/journals/JIS/`. (Cited on page 206.)

[96] Jean-Guillaume Dumas, Thierry Gautier, Pascal Giorgi, Jean-Louis Roch, and Gilles Villard. *Givaro-3.2.13rc1: C++ library for arithmetic and algebraic computations*, September 2008. `http://ljk.imag.fr/CASYS/LOGICIELS/givaro/`. (Cited on pages 21, 168, 210, and 346.)

[97] Andreas Enge. *Elliptic Curves and Their Applications to Cryptography: An Introduction.* Springer, 1st edition, August 1999. (Cited on page 224.)

[98] F. J. MacWilliams and N. J. Sloane. The theory of error-correcting codes. In *Amsterdam, North Holland*, 1977. (Cited on pages 11, 115, 116, and 152.)

[99] J.-C. Faugère and G. Ars. An Algebraic Cryptanalysis of Nonlinear Filter Generators using Gröbner bases. In *Rapport de Recherche INRIA*, pages 4739–2003, 2003. (Cited on page 61.)

[100] Keqin Feng, Qunying Liao, and Jing Yang. Maximal values of generalized algebraic immunity. *Des. Codes Cryptography*, 50(2):243–252, 2009. (Cited on page 88.)

[101] J-P Flori and S. Mesnager. Hyper-bent functions of the Mesnager family and hyperelliptic curves. Preprint. (Cited on pages 193, 236, 237, 244, and 246.)

[102] J-P Flori and S. Mesnager. Dickson polynomials, hyperelliptic curves and hyper-bent functions. In *7th International conference SETA 2012, LNCS 7280, Springer*, pages 40–52, 2012. (Cited on pages 2, 26, 53, 54, 55, 192, 193, 237, 244, 329, and 351.)

[103] J-P. Flori, S. Mesnager, and G. Cohen. Binary Kloosterman sums with value 4. In Liqun Chen, editor, *IMA Int. Conf.*, volume 7089 of *Lecture Notes in Computer Science*, pages 61–78. Springer, 2011. (Cited on pages 26 and 351.)

[104] J-P. Flori, H. Randriam, G. Cohen, and S. Mesnager. On a conjecture about binary strings distribution. In C. Carlet and A. Pott, editors, *SETA*, volume 6338 of *Lecture Notes in Computer Science*, pages 346–358. Springer, 2010. (Cited on pages 11, 96, 97, 98, 99, and 336.)

[105] Jean-Pierre Flori. PhD Thesis, Telecom ParisTech. 2012. (Cited on pages 94, 95, 96, and 335.)

[106] Jean-Pierre Flori and Hugues Randriam. On the number of carries occurring in an addition mod $2^k - 1$. In *Journal Integers, vol 12*, 2012. (Cited on pages 9, 94, 96, 97, and 335.)

[107] R. Forré. A fast correlation attack on nonlinearly feedforward filtered shift register sequences. . In *Proceedings of EUROCRYPT '89, Lecture Notes in Computer Science, 434*, pages 586–595, 1990. (Cited on page 60.)

[108] Mireille Fouquet, Pierrick Gaudry, and Robert Harley. An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15(4):281–318, 2000. (Cited on page 252.)

[109] Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2011. `http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html`. (Cited on page 224.)

[110] Kseniya Garaschuk and Petr Lisoněk. On binary Kloosterman sums divisible by 3. *Des. Codes Cryptography*, 49(1-3):347–357, 2008. (Cited on page 250.)

[111] D. Glynn. Two new sequences of ovals in finite Desarguesian planes of even order. In *Lecture Notes in Mathematics 1036.* (Cited on pages 15, 138, 340, and 341.)

[112] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. In *IEEE Trans. Inform. Theory 14 (1)*, pages 154–156, 1968. (Cited on pages 27, 107, 255, and 352.)

[113] J. Golic. Fast low order approximation of cryptographic functions. In *EUROCRYPT 1996. Lecture notes in Computer Science, vol. 1070. Spinger-Verlag*, pages 268–282, 1996. (Cited on pages 6, 79, and 333.)

[114] F. Gologlu. Almost Bent and Almost Perfect Nonlinear Functions, Exponential Sums, Geometries and Sequences. In *PhD dissertation, University of Magdeburg*, 2009. (Cited on pages 180 and 281.)

[115] G. Gong and S. W. Golomb. Transform Domain Analysis of DES. In *IEEE Trans. Inform. Theory, Vol. 45. no. 6*, pages 2065–2073, 1999. (Cited on pages 20 and 345.)

[116] Guang Gong and Solomon Wolf Golomb. Transform domain analysis of DES. *IEEE Transactions on Information Theory*, 45(6):2065–2073, 1999. (Cited on page 152.)

[117] B. Guo and Y. Yang. Further enumerating Boolean functions of cryptographic significance 8. In *Journal of Cryptology*, pages 115–122, 1995. (Cited on page 69.)

[118] Faruk Göloğlu, Petr Lisoněk, Gary McGuire, and Richard Moloney. Binary Kloosterman sums modulo 256 and coefficients of the characteristic polynomial. *Information Theory, IEEE Transactions on*, PP(99):1, 2012. (Cited on page 249.)

[119] Faruk Göloğlu, Gary McGuire, and Richard Moloney. Binary Kloosterman sums using Stickelberger's theorem and the Gross-Koblitz formula. *Acta Arith.*, 148(3):269–279, 2011. (Cited on page 249.)

[120] F. Harary and E. M. Palmer. Graphical Enumeration. In *Academic, New York*, 1973. (Cited on page 71.)

[121] Robert Harley. Asymptotically optimal p-adic point-counting. Email to NMBRTHRY list, December 2002. `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=nmbrthry&T=0&P=1343`. (Cited on pages 251 and 252.)

[122] P. Hawkes and G. Rose. Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers. In *Proceedings of CRYPTO 2004, Lecture Notes in Computer Science 3152*, pages 390–406, 2004. (Cited on page 61.)

[123] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37(145):27–38, 1986. (Cited on page 205.)

[124] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. In *Discr. Math, vol. 16*, pages 209–232, 1976. (Cited on pages 27, 255, and 352.)

[125] T. Helleseth. Correlation of m-sequences and related topics. In *Proc. SETA[U+FFFD]8, Discrete Mathematics and Theoretical Computer Science, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer*, pages 49–66, 1999. (Cited on pages 27, 255, and 352.)

[126] T. Helleseth, A. Kholosha, and S. Mesnager. Niho Bent Functions and Subiaco/Adelaide Hyperovals. In *Proceedings of the 10-th International Conference on Finite Fields and Their Applications (Fq'10), Contemporary Math., AMS. Vol 579*, pages 91–101, 2012. (Cited on pages 19, 141, and 345.)

[127] T. Helleseth and P. V. Kumar. Sequences with low correlation. In *Handbook of Coding Theory, Part 3: Applications, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, chapter. 21*, pages 1765–1853, 1998. (Cited on pages 27, 255, and 352.)

[128] Tor Helleseth and Victor Zinoviev. On Z_4 linear Goethals codes and Kloosterman sums. *Des. Codes Cryptography*, 17(1-3):269–288, 1999. (Cited on page 249.)

[129] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967. (Cited on page 205.)

[130] X. D. Hou. Some results on the covering radii of Reed-Muller codes. In *IIEEE Transactions on Information Theory, Vol. 39, no. 2*, 1993. (Cited on pages 31, 285, 286, and 355.)

[131] X. D. Hou. $GL(m, 2)$ acting on $R(r, m)/R(r-1, m)$. In *Discrete Mathematics, Vol. 149*, pages 99–122, 1996. (Cited on pages 31, 285, and 355.)

[132] X.-D. Hou and P. Langevin. Results on bent functions. In *Journal of Combinatorial Theory, Series A, 80*, pages 232–246, 1997. (Cited on page 111.)

[133] H. Hu and D. Feng. W. Cherowitzo. α-flocks and hyperovals. In *Geometriae Dedicata*, pages 221–246, 1998. (Cited on pages 15, 138, and 341.)

[134] H. Hu and D. Feng. On quadratic bent functions in polynomial forms. In *IEEE Trans. Inform. Theory 53 (7)*, pages 2610–2615, 2007. (Cited on page 108.)

[135] Hendrik Hubrechts. Point counting in families of hyperelliptic curves in characteristic 2. *LMS J. Comput. Math.*, 10:207–234, 2007. (Cited on pages 224 and 247.)

[136] The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. `http://oeis.org`. (Cited on pages 205 and 206.)

[137] T. Iwata and K. Kurosawa. Probabilistic higher order differential attack and higher order bent functions. In *ASIACRYPT 1999. Lecture notes in Computer Science, vol. 1716. Spinger-Verlag*, pages 62–74, 1999. (Cited on pages 6, 79, and 333.)

[138] Qingfang Jin, Zhuojun Liu, and Baofeng Wu. 1-resilient Boolean function with optimal algebraic immunity. Cryptology ePrint Archive, Report 2011/549, 2011. `http://eprint.iacr.org/`. (Cited on pages 9 and 93.)

[139] Qingfang Jin, Zhuojun Liu, Baofeng Wu, and Xiaoming Zhang. A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity. Cryptology ePrint Archive, Report 2011/515, 2011. `http://eprint.iacr.org/`. (Cited on pages 9, 92, 93, 96, and 335.)

[140] T. Johansson and F. Jönsson. Fast correlation attacks based on turbo code techniques. In *Advances in Cryptology - CRYPTO'99, no. 1666 in Lecture Notes in Computer Science*, pages 181–197, 1999. (Cited on page 60.)

[141] T. Johansson and F. Jönsson. Improved fast correlation attack on stream ciphers via convolutional codes. In *Proceedings of EUROCRYPT'99, Lecture Notes in Computer Science, 1592*, pages 347–362, 1999. (Cited on page 60.)

[142] T. Johansson and F. Jönsson. Fast correlation attacks through reconstruction of linear polynomials. In *Advances in Cryptology - CRYPTO 2000, no. 1880 in Lecture Notes in Computer Science*, pages 300–315, 2000. (Cited on page 60.)

[143] T. Iwata K. Kurosawa and T. Yoshiwara. New covering radius of Reed-Muller codes for t-resilient functions. In *SAC 2001 ser. Lecture notes in computer science, Vol. 2259, Springer-Verlag*, pages 75–86, 2001. (Cited on pages 31 and 356.)

[144] T. Kasami. Weight enumerators for several classes of subcodes of the 2nd-order Reed-Muller codes. In *Information control, Vol 18*, pages 369–394, 1971. (Cited on page 108.)

[145] T. Kasami and N. Tokura. On the weight structure of Reed-Muller codes. In *IIEEE Transactions on Information Theory, Vol. 16*, pages 752–759, 1970. (Cited on pages 291, 294, 295, and 304.)

[146] Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris. I Math.*, 309(11):723–726, 1989. (Cited on pages 25, 223, 225, and 350.)

[147] Pin-Hui Ke, Jie Zhang, and Qiao-Yan Wen. Further constructions of almost resilient functions. In *Cryptology ePrint Archive, Report 2005/453*, 2005. (Cited on page 66.)

[148] Kiran Sridhara Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001. (Cited on page 224.)

[149] K. Khoo, G. Gong, and D. R. Stinson. A new family of Gold-like sequences. In *IEEE Trans. Inform. Theory Lausanne, Switzerland*, page 181, 2002. (Cited on pages 27, 255, and 352.)

[150] K. Khoo, G. Gong, and D. R. Stinson. A new characterization of semibent and bent functions on finite fields. In *Des. Codes. Cryptogr. vol. 38, no. 2*, pages 279–295, 2006. (Cited on pages 27, 255, and 352.)

[151] S. H. Kim and J. S. No. New families of binary sequences with low correlation. In *IEEE Trans. Inform. Theory, vol. 49, no. 11*, pages 3059–3065, 2003. (Cited on page 108.)

[152] L. Knudsen and M. Robshaw. Non-linear approximations in linear cryptanalysis. In *Advances in Cryptology. Eurocrypt 1996.* (Cited on pages 6, 31, 79, 333, and 356.)

[153] Neal Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In Alfred John Menezes and Scott Alexander Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 1990. (Cited on page 223.)

[154] K. Kurosawa, T. Johansson, and D. Stinson. Almost k-wise Independent Sample Spaces and Their Cryptologic Applications. In *Journal of Cryptology, 14(4)*, pages 301–324, 2001. (Cited on page 66.)

[155] K. Kurosawa and R. Matsumoto. Almost Security of Cryptographic Boolean Functions. In *IEEE Transactions on Information Theory, Vol 50 no.11*, pages 2752–2761, 2004. (Cited on pages 3, 62, 65, and 331.)

[156] G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. In *IEEE Trans. Inform. Theory 36 (3)*, pages 686–692, 1990. (Cited on pages 43, 45, 107, 155, and 237.)

[157] Gilles Lachaud and Jacques Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987. (Cited on pages 25, 225, and 350.)

[158] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate. (Cited on page 223.)

[159] G. Leander. Monomial Bent Functions. In *IEEE Trans. Inform. Theory (52) 2*, pages 738–743, 2006. (Cited on pages 20, 45, 107, 108, 154, 155, 166, 170, 280, and 345.)

[160] G. Leander and A. Kholosha. Bent functions with 2^r Niho exponents. In *IEEE Trans. Inform. Theory 52 (12)*, pages 5529–5532, 2006. (Cited on pages 13, 14, 108, 109, 125, 138, 258, 281, 338, and 339.)

[161] Philip A. Leonard and Kenneth S. Williams. Quartics over GF(2^n). *Proc. Amer. Math. Soc.*, 36:347–350, 1972. (Cited on pages 25 and 350.)

[162] Reynald Lercier and David Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. *Ramanujan J.*, 12(3):399–423, 2006. (Cited on page 225.)

[163] Reynald Lercier, David Lubicz, and Frederik Vercauteren. Point counting on elliptic and hyperelliptic curves. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 407–453. Chapman & Hall/CRC, Boca Raton, FL, 2006. (Cited on page 251.)

[164] Na Li and Wen-Feng Qi. Construction and analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 84–98. Springer, 2006. (Cited on pages 8, 86, and 334.)

[165] Na Li, Longjiang Qu, Wen-Feng Qi, GuoZhu Feng, Chao Li, and DuanQiang Xie. On the construction of Boolean functions with optimal algebraic immunity. *IEEE Transactions on Information Theory*, 54(3):1330–1334, 2008. (Cited on pages 8, 86, and 334.)

[166] R. Lidl and H. Niederreiter. Finite fields. In *Encyclopedia of mathematics and its applications 20, Cambridge University Press*, 1997. (Cited on page 128.)

[167] Rudolf Lidl, Gary Lee Mullen, and Gerhard Turnwald. *Dickson polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993. (Cited on pages 54 and 55.)

[168] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn. (Cited on page 55.)

[169] Petr Lisoněk. On the connection between Kloosterman sums and elliptic curves. In Solomon Wolf Golomb, Matthew Geoffrey Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 182–187. Springer, 2008. (Cited on pages 250 and 251.)

[170] Petr Lisoněk. An efficient characterization of a family of hyperbent functions. *IEEE Transactions on Information Theory*, 57(9):6010–6014, 2011. (Cited on pages 25, 193, 228, 229, 237, 238, 244, 246, 274, and 350.)

[171] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. In *Cryptology ePrint Archive, Report 2005/441*, 2005. (Cited on pages 85 and 86.)

[172] Mikhail Sergeevich Lobanov. Exact relations between nonlinearity and algebraic immunity. *Diskretn. Anal. Issled. Oper.*, 15(6):34–47, 95, 2008. (Cited on pages 8, 86, and 334.)

[173] W. Ma, M. Lee, and F. Zhang. A new class of bent functions. In *IEICE Trans. Fundamentals, Vol E88-A , Issue 7*, pages 2039–2040, 2005. (Cited on page 108.)

[174] D. J. C. MacKay. Information Theory, Inference, and Learning Algorithms. In *Cambridge University Press*, 2003. (Cited on page 64.)

[175] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16. (Cited on pages 89 and 285.)

[176] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes. II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16. (Cited on pages 27, 89, and 352.)

[177] S. Maitra and P. Sarkar. Enumeration of correlation immune Boolean functions. In *ACISP*, pages 12–25, 1999. (Cited on page 69.)

[178] A. Maschietti. Difference sets and hyperovals. In *Designs, Codes and Cryptography 14*, pages 89–98, 1998. (Cited on page 138.)

[179] J. L. Massey. Shift-register analysis and BCH decoding. In *IEEE Transactions on Information Theory, vol. 15*, pages 122–127, 1969. (Cited on page 11.)

[180] James Lee Massey. Shift-register synthesis and BCH decoding. *Information Theory, IEEE Transactions on*, 15(1):122 – 127, jan 1969. (Cited on page 59.)

[181] M. Matsui. Linear cryptanalysis method for DES cipher. In *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 386–397, 1994. (Cited on pages 18, 113, and 338.)

[182] M. Matsui. Linear cryptanalysis method for DES cipher. In *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 386–397, 1994. (Cited on pages 27, 60, 255, and 351.)

[183] Mitsuru Matsui. Linear cryptoanalysis method for DES cipher. In *EUROCRYPT*, pages 386–397, 1993. (Cited on page 102.)

[184] Mitsuru Matsui and Atsuhiro Yamagishi. A new method for known plaintext attack of FEAL cipher. In *EUROCRYPT*, pages 81–91, 1992. (Cited on page 102.)

[185] R. L. McFarland. A family of noncyclic difference sets. In *Journal of Comb. Theory, Series A, no. 15*, pages 1–10, 1973. (Cited on page 106.)

[186] A. McLoughlin. The covering radius of the $(m-3)$-rd order Reed-Muller codes and a lower bound on the $(m-4)$-th order Reed-Muller code. In *SIAM J. Appl. Math., vol. 37, no. 2*, pages 419–422, 1979. (Cited on pages 31, 285, and 355.)

[187] W. Meier, E. Pasalic, and C. Carlet. Algebraic attacks and decomposition of Boolean functions. In *Eurocrypt 2004, ser. Lecture notes in Computer Science, vol. 3027. Spinger-Verlag*, pages 474–491, 2004. (Cited on pages 2, 31, 60, 63, 330, and 356.)

[188] W. Meier and O. Staffelbach. Fast correlation attacks on stream ciphers. In *Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science 330*, pages 301–314, 1988. (Cited on pages 27, 60, 255, and 351.)

[189] Willi Meier, Enes Pasalic, and Claude Carlet. Algebraic attacks and decomposition of Boolean functions. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 474–491. Springer, 2004. (Cited on page 61.)

[190] Willi Meier and Othmar Staffelbach. Fast correlation attacks on stream ciphers (extended abstract). In *EUROCRYPT*, pages 301–314, 1988. (Cited on page 60.)

[191] Alfred John Menezes, Paul C. van Oorschot, and Scott Alexander Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. (Cited on pages 58 and 59.)

[192] S. Mesnager. Hyper-bent boolean functions with multiple trace terms. In *Proceedings of International Workshop on the Arithmetic of Finite Fields. M.A. Hasan and T.Helleseth (Eds.): WAIFI 2010, LNCS 6087, pp. 97–113. Springer, Heidelberg (2010).* (Cited on pages 25, 181, 182, 183, 184, 185, 186, 187, 193, 197, 211, 348, and 349.)

[193] S. Mesnager. Improving the Lower Bound on the Higher Order Nonlinearity of Boolean Functions With Prescribed Algebraic Immunity. In *IEEE Transactions on Information Theory Vol. 54, no. 8*, pages 3656–3662, 2008. (Cited on pages 10, 80, 81, 83, 84, 85, and 336.)

[194] S. Mesnager. On the number of resilient Boolean functions. In *Journal of Number Theory and its Applications, Vol. 5*, pages 139–153, 2008. (Cited on pages 10, 72, 73, 74, 75, 76, 77, 78, and 336.)

[195] S. Mesnager. A new class of bent boolean functions in polynomial forms. In *Proceedings of international Workshop on Coding and Cryptography, WCC 2009*, pages 5–18, 2009. (Cited on pages 22, 155, 156, 157, 170, 172, 187, 280, and 347.)

[196] S. Mesnager. A new family of hyper-bent boolean functions in polynomial form. In *Proceedings of Twelfth International Conference on Cryptography and Coding, Cirencester, United Kingdom. M. G. Parker (Ed.): IMACC 2009, LNCS 5921, Springer, Heidelberg*, pages 402–417, 2009. (Cited on pages 2, 22, 170, 171, 172, 174, 175, 176, 177, 181, 187, 280, 281, 329, and 347.)

[197] S. Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. In *journal Design, Codes and Cryptography, 59(1-3)*, pages 265–279, 2011. (Cited on pages 22, 156, 157, 161, 166, 170, 176, 177, 181, 193, 211, 280, 281, and 347.)

[198] S. Mesnager. Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. *IEEE Transactions on Information Theory*, 57(9):5996–6009, 2011. (Cited on pages 25, 158, 159, 162, 163, 187, 188, 190, 191, 280, and 349.)

[199] S. Mesnager. Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. In *IEEE Transactions on Information Theory-IT, Vol 57, No 11*, pages 7443–7458, 2011. (Cited on pages 2, 28, 30, 46, 49, 51, 52, 256, 257, 258, 261, 262, 263, 265, 267, 270, 271, 273, 329, 353, and 355.)

[200] S. Mesnager. Semi-bent functions with multiple trace terms and hyperelliptic curves. In *Proceeding of International Conference on Cryptology and Information Security in Latin America (IACR), Latincrypt 2012, LNCS 7533, Springer*, pages 18–36, 2012. (Cited on pages 30, 274, 275, and 355.)

[201] S. Mesnager and G. Cohen. On the link of some semi-bent functions with Kloosterman sums. In *Prooceding of International Workshop on Coding and Cryptology, Y.M. Chee et al. (Eds.): IWCC 2011, LNCS 6639, Springer*, pages 263–272, 2011. (Cited on pages 28, 30, 256, 352, and 355.)

[202] S. Mesnager and J-P Flori. On hyper-bent functions via Dillon-like exponents. In *IEEE Internaional Symposium on Information Theory, IMT, Cambridge, MA, USA, July 1–6*. (Cited on pages 1, 25, and 349.)

[203] M.J. Mihaljevic, M.P.C. Fossorier, and H.Imai. A Low-Complexity and High-Performance Algorithm for the Fast Correlation Attack. In *B. Schneier, editor, FSE 2000, volume 1978 of Lecture Notes in Computer Science, Springer-Verlag*, pages 196–210, 2001. (Cited on page 63.)

[204] W. Millan. Low order approximations of cipher functions. In *ser. Lecture notes in Computer Science. Springer-Verlag, vol. 1029*, pages 144–155, 1996. (Cited on pages 6, 79, and 333.)

[205] C. J. Mitchell. Enumerating Boolean functions of cryptographic significance. In *Journal of Cryptology 2*, pages 155–170, 1990. (Cited on page 69.)

[206] H. Molland, J.E. Mathiassen, and T.Helleseth. Improved fast correlation attack using low rate codes. In *Cryptography and Coding, volume 2898 of Lecture Notes in Computer Science, Springer-Verlag GmbH*, pages 67–81, 2003. (Cited on page 63.)

[207] Richard Moloney. *Divisibility Properties of Kloosterman Sums and Division Polynomials for Edward Curves*. PhD thesis, University College Dublin, may 2011. (Cited on page 249.)

[208] Michael Burnett Monagan, Keith Oliver Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron, and Paul DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005. (Cited on page 98.)

[209] J. Mykkeltveit. The covering radius of the (128, 8) reed-muller code is 56. In *IEEE Transactions on Information Theory 26*, pages 359–362, 1980. (Cited on pages 27 and 352.)

[210] Y. Niho. Multi-valued cross-correlation functions between two maximal linear recursive sequences. In *Ph.D. dissertation, Univ. Sothern Calif., Los Angeles*, 1972. (Cited on pages 27, 255, and 352.)

[211] K. Nyberg. Perfect non-linear S-boxes. In *Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science 547*, pages 378–386, 1992. (Cited on pages 18, 113, 338, and 344.)

[212] K. Nyberg. On the construction of highly nonlinear permutations. In *Proceedings of EUROCRYPT'92, Lecture Notes in Computer Science 658*, pages 92–98, 1993. (Cited on pages 18 and 338.)

[213] K. Nyberg. New bent mappings suitable for fast implementation. In *of Fast Software Encryption 1993, Lecture Notes in Computer Science 809*, pages 179–184, 1994. (Cited on page 115.)

[214] Christine M. O'Keefe and Tim Penttila. Polynomials representing hyperovals. In *Tech. Report 26, Department of Mathematics, University of Western Australia*, 1989. (Cited on page 148.)

[215] P. Rabizzoni P. Veron P. Langevin, G. Leander and J.-P. Zanotti. Counting all bent functions in dimension eight 99270589265934370305785861242880. In *Des. Codes Cryptography 59 (1–3)*, pages 193–205, 2011. (Cited on pages 12 and 105.)

[216] The PARI Group, Bordeaux. *PARI/GP, version* `2.4.3`, October 2010. available from `http://pari.math.u-bordeaux.fr/`. (Cited on page 252.)

[217] Hwasin Park, Joongsoo Park, and Daeyeoul Kim. A criterion on primitive roots modulo p. *J. KSIAM*, 4(1):29–38, 2000. (Cited on page 205.)

[218] M.G. Parker and A. Pott. On Boolean Functions Which Are Bent and Negabent. In *nt. Work- shop on Sequences, Subsequences, and Consequences (SSC 2007), Los Angeles, USA, 2007. Revised Invited Papers, Golomb, S.W., Gong, G., Helleseth, T., and Song, H.-Y., Eds., Lect. Notes Comp. Sci. 4893*, pages 9–23, 2007. (Cited on pages 27 and 351.)

[219] S. E. Payne. Ovali e curve σ nei piani di Galois di caratteristica due. In *Atti dell' Accad. Naz. Lincei Rend. 32 8*, pages 785–790, 1962. (Cited on pages 15, 138, and 340.)

[220] S. E. Payne. Multivalued cross-correlation functions between two maximal linear recursive sequences. In *PhD thesis, Univ. of Southern California*, 1972. (Cited on pages 13 and 108.)

[221] S. E. Payne. A new infinite family of generalized quadrangles. In *Congr. Numer. 49*, pages 115–128, 1985. (Cited on pages 15, 138, and 341.)

[222] Stanley E. Payne, Tim Penttila, and Ivano Pinneri. Isomorphisms between Subiaco q-clan geometries. In *Bull. Belg. Math. Soc. Simon Stevin 2, no. 2*, pages 197–222, 1995. (Cited on page 142.)

[223] C. Qu, J. Seberry, and J. Pieprzyk. Homogeneous Bent Functions. In *Discrete Appl. Math 102 no. 1-2*, pages 133–139, 2000. (Cited on pages 27 and 351.)

[224] G. L. Mullen R. Lidl and G. Turnwald. Dickson Polynomials. In *ser.Pitman Monographs in Pure and Applied Mathematics. Reading, MA: Addison-Wesley, vol. 65*, 1993. (Cited on pages 15, 53, 138, 140, 341, and 342.)

[225] Kalle Ranto. On algebraic decoding of the z4-linear goethals-like codes. *IEEE Transactions on Information Theory*, 46(6):2193–2197, 2000. (Cited on page 53.)

[226] S. Rønjom and T. Helleseth. A new attack on the filter generator. In *IEEE Transactions on Information Theory, vol. 53, no. 5*, pages 1752–1758, 2007. (Cited on pages 11, 59, 105, and 330.)

[227] O.S. Rothaus. On "bent" functions. In *J. Combin.Theory Ser A 20*, pages 300–305, 1976. (Cited on pages 11, 26, 89, 102, 105, 110, 336, and 351.)

[228] Oscar Seymour Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976. (Cited on page 89.)

[229] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000. (Cited on page 251.)

[230] J. Schatz. The second-order Reed-Muller code of length 64 has covering radius 18. In *IEEE Transactions on Information Theory, Vol. IT-27, no. 4*, pages 529–530, 1981. (Cited on pages 31, 285, 286, and 355.)

[231] M. Schneider. A note on the construction and upper bounds of correlation-immune functions. In *6th IMA Conference*, pages 295–306, 1997. (Cited on pages 69 and 71.)

[232] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Comb. Theory, Ser. A*, 46(2):183–211, 1987. (Cited on page 223.)

[233] C.E. Shannon. Communication theory of secrecy systems. In *Bell system technical journal, 28*, pages 656–715, 1949. (Cited on pages 58, 61, and 330.)

[234] T. Shimoyama and T. Kaneko. Quadratic relation of s-box and its application to the linear attack of full round aes. In *CRYPTO 1998, ser. Lecture Notes in Computer Science, vol. 1462, ser. Lecture Notes in Computer Science*, pages 200–211, 1998. (Cited on pages 31, 79, and 356.)

[235] Victor Shoup. NTL 5.4.2: A library for doing number theory, March 2008. `www.shoup.net/ntl`. (Cited on pages 21, 168, and 346.)

[236] T. Siegenthaler. Correlation-immunity of nonlinear combining boolean fucntions for cryptographic applications. In *IEEE Transactions on Information Theory, Vol 30, no. 5*, pages 776–779, 1984. (Cited on pages 2, 3, 61, 62, 70, and 330.)

[237] T. Siegenthaler. Decrypting a Class of Stream Ciphers Using Ciphertext. In *IEEE Transactions on Computer, vol. C-34, no 1*, pages 81–85, 1985. (Cited on pages 60 and 61.)

[238] Joseph Hillel Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. (Cited on page 222.)

[239] N. J. Sloane. Unsolved problems related to the covering radius of codes. In *Open problems in Communication and Computation, 1987, ed. T. M. Cover and Gopinath, Springer-Verlag, NY*, 1987. (Cited on pages 31, 285, and 355.)

[240] S. H. Sung S.M. Park, S. Lee and K. Kim. Improving bounds for the number of correlation-immune Boolean functions. In *Information Processing Letters 61*, pages 209–212, 1997. (Cited on page 69.)

[241] William Arthur Stein et al. *Sage Mathematics Software (Version 4.7)*. The Sage Development Team, 2011. `http://www.sagemath.org`. (Cited on pages 21, 99, 168, 210, 252, and 346.)

[242] G. Sun and C.Wu. Construction of Semi-Bent Boolean Functions in Even Number of Variables. In *Chinese Journal of Electronics, vol 18, No 2*, 2009. (Cited on pages 27, 255, and 352.)

[243] N. Tokura T. Kasami and S. Azumi. On the weight enumeration of weights less than $2.5d$ of Reed-Muller codes. In *Information and Control, vol. 30*, pages 380–395, 1976. (Cited on pages 294, 295, and 304.)

[244] T. Satoh, T. Iwata and K. Kurosawa. On cryptographically secure vectorial Boolean functions. In *Proceedings of Asiacrypt 1999, Lecture Notes in Computer Science 1716*, pages 20–28, 1999. (Cited on page 114.)

[245] D. Tang, C. Carlet, and X. Tang. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. Cryptology ePrint Archive, Report 2011/366, 2011. `http://eprint.iacr.org/`. To appear in IEEE- IT. (Cited on pages 9, 10, 88, 91, 92, 96, 335, and 336.)

[246] X. Tang, D. Tang, X. Zeng, and L. Hu. Balanced Boolean functions with (almost) optimal algebraic immunity and very high nonlinearity. Cryptology ePrint Archive, Report 2010/443, 2010. `http://eprint.iacr.org/`. (Cited on pages 9, 90, 92, and 334.)

[247] Ziran Tu and Yingpu Deng. Boolean functions with all main cryptographic properties. Cryptology ePrint Archive, Report 2010/518, 2010. `http://eprint.iacr.org/`. (Cited on pages 90 and 93.)

[248] Ziran Tu and Yingpu Deng. A class of 1-resilient function with high nonlinearity and algebraic immunity. Cryptology ePrint Archive, Report 2010/179, 2010. `http://eprint.iacr.org/`. (Cited on pages 9, 90, and 334.)

[249] Ziran Tu and Yingpu Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Des. Codes Cryptography*, 60(1):1–14, 2011. (Cited on pages 8, 9, 88, 89, 90, 91, 92, 96, 97, 334, and 335.)

[250] `Pynac.sagemath.net`. *Pynac, symbolic computation with Python objects (Version 0.2.2)*, 2011. `http://pynac.sagemath.org`. (Cited on page 210.)

[251] T. Johansson V. V. Chepyzhov and B. Smeets. A simple algorithm for fast correlation attacks on stream ciphers. In *B. Schneier, editor, FSE 2000, volume 1978 of Lecture Notes in Computer Science, Springer-Verlag, April 10-12*, pages 181–195, 2001. (Cited on pages 2, 4, 60, 63, 64, 330, and 331.)

[252] Jacobus Hendrikus van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999. (Cited on page 89.)

[253] Frederik Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2003. (Cited on pages 224 and 235.)

[254] Frederik Vercauteren. Advances in point counting. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 103–132. Cambridge Univ. Press, Cambridge, 2005. (Cited on page 251.)

[255] Frederik Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2007. (Cited on pages 251 and 252.)

[256] Baocheng Wang, Chunming Tang, Yanfeng Qi, and Yixian Yang. A generalization of the class of hyper-bent boolean functions in binomial forms. Cryptology ePrint Archive, Report 2011/698, 2011. `http://eprint.iacr.org/`. (Cited on pages 177 and 212.)

[257] Baocheng Wang, Chunming Tang, Yanfeng Qi, Yixian Yang, and Maozhi Xu. A new class of hyper-bent boolean functions in binomial forms. *CoRR*, abs/1112.0062, 2011. (Cited on pages 53, 177, and 212.)

[258] Baocheng Wang, Chunming Tang, Yanfeng Qi, Yixian Yang, and Maozhi Xu. A new class of hyper-bent Boolean functions with multiple trace terms. Cryptology ePrint Archive, Report 2011/600, 2011. `http://eprint.iacr.org/`. (Cited on pages 24, 192, 193, 212, 213, and 349.)

[259] Qichun Wang and Thomas Johansson. A note on fast algebraic attacks and higher order nonlinearities. In Xuejia Lai, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology*, volume 6584 of *Lecture Notes in Computer Science*, pages 404–414. Springer Berlin / Heidelberg, 2011. 10.1007/978-3-642-21518-6-28. (Cited on pages 9, 91, and 335.)

[260] Qichun Wang, Jie Peng, Haibin Kan, and Xiangyang Xue. Constructions of cryptographically significant Boolean functions using primitive polynomials. *IEEE Transactions on Information Theory*, 56(6):3048–3053, 2010. (Cited on page 88.)

[261] William Charles Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969. (Cited on page 223.)

[262] C.M. O'Keefe W.E. Cherowitzo and T. Penttila. W. Cherowitzo, T. Penttila, I. Pinneri and G. F. Royle. Flocks and ovals. In *Geometriae Dedicata, 60, no. 1*, pages 17–37, 1996. (Cited on pages 15, 138, and 341.)

[263] C.M. O'Keefe W.E. Cherowitzo and T. Penttila. A unified construction of finite geometries associated with q-clans in characteristic two. In *Advances in Geometry, 3*, pages 1–21, 2003. (Cited on pages 15, 138, and 341.)

[264] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948. (Cited on pages 25 and 350.)

[265] Christine M. O'Keefe William E. Cherowitzo and Tim Penttila. A unified construction of finite geometries associated with q-clans in characteristic 2. In *Adv. Geom (3) no. 1*, pages 1–21, 2003. (Cited on page 148.)

[266] G-Z Xiao and J.L. Massey. A spectral characterization of correlation-immune combining functions. In *IEEE Transactions on Information Theory, Vol 34 no. 3*, pages 569–571, 1988. (Cited on pages 3 and 61.)

[267] C. Ding Xiao Guo-Zhen and W. Shan. The stability theory of stream ciphers. In *Lecture Notes in Computer Science 561*, 1991. (Cited on page 60.)

[268] N. Manev Y. Borissov and S. Nikova. On the non-minimal codewords in binary Reed-Muller codes. In *international workshop on the coding and cryptography (WCC 2001)Discrete Appl. Math*, pages 65–74, 2003. (Cited on page 298.)

[269] Y. X. Yang and B. Guo. Further enumerating Boolean funvtions of cryptographic significance. In *Journal of Cryptology, 8*, pages 115–122, 1995. (Cited on page 69.)

[270] Kim-Ee Yeoh. GP/Pari implementation of point counting in characteristic 2. `http://pages.cs.wisc.edu/~yeoh/nt/satoh-fgh.gp`. (Cited on page 252.)

[271] A. M. Youssef and G. Gong. Hyper-Bent Functions. In *Advances in Crypology – Eurocrypt'01*, LNCS, pages 406–419. Springer, 2001. (Cited on pages 20, 27, 345, and 351.)

[272] Amr Mohamed Youssef and Guang Gong. Hyper-bent functions. In Birgit Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 406–419. Springer, 2001. (Cited on pages 151 and 153.)

[273] N. Y. Yu and G. Gong. Construction of quadratic Bent functions in polynomial forms. In *IEEE Trans. Inform. Theory (52) 7*, pages 3291–3299, 2006. (Cited on page 108.)

[274] Jian-Zhoua Zhang, Zhi-Shenga You, and Zheng-Liang Li. Enumeration of binary orthogonal arrays of strength 1. Discrete Mathematics, 239. In *Journal of Cryptology, 14(4)*, pages 191–198, 2001. (Cited on page 69.)

[275] Y. Zheng and X. M. Zhang. Plateaued functions. In *Advances in Cryptology-ICICS 1999, vol 1726 Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag*, pages 284–300, 1999. (Cited on pages 27, 255, and 351.)

[276] Y. Zheng and X. M. Zhang. Relationships between bent functions and complementary plateaued functions. In *Lecture Notes in Computer Science, vol 1787*, pages 60–75, 1999. (Cited on pages 27, 255, and 351.)

Index

Résumé long

Résumé des chapitres

Chapitres 1 et 2

Dans le chapitre 1, nous effectuons un certain nombre de rappels sur les fonctions booléennes, en rappelant notamment leurs différentes représentations, et fixons les principales notations que nous utilisons dans les chapitres suivants.

Dans le chapitre 2, nous introduisons la transformée de Walsh des fonctions booléennes en rappelant certaines de ses propriétés. Nous y rappelons aussi un certain nombre de résultats sur les sommes de Kloosterman et cubiques.

Nous fournissons plusieurs résultats techniques sur certaines sommes exponentielles et des outils mathématiques dont nous avons besoin par la suite dans le Chapitre 5, Chapitre 7 et Chapitre 8. Plus précisément, d'une part, nous sommes intéressés à exprimer certaines sommes exponentielles particulières sur le cercle unité de $\mathbb{F}_{2^n}$ (c'est -à- dire le groupe cyclique des racines 2^m+1-èmes de l'unité de $\mathbb{F}_{2^n}$) en termes de sommes de Kloosterman et des sommes cubiques. De telles expressions seront utilisées pour exhiber des conditions du caractère hyper-courbe et semi-courbe de certaines fonctions booléennes dans en formes polynomiales faisant intervenir des sommes de Kloosterman et sommes cubiques. Enfin nous étudions l'action des polynômes de Dickson sur des sous-ensembles de corps finis liée à la trace de l'inverse d'un élément et nous fournissons une autre preuve d'un résultat qui n'est pas si bien connu. Ces résultats sont ensuite appliqués à l'étude des familles de fonctions booléennes et aux caractérisations de leur caractère hyper-courbe en termes de sommes exponentielles.

Publications

Certains des résultats présentés dans le chapitre 2 sont tirés des publications suivantes :

- S. Mesnager. A new family of hyper-bent Boolean functions in polynomial form. Proceedings of Twelfth International Conference on Cryptography and Coding. Cirencester, United Kingdom. M. G. Parker (Ed.) IMACC 2009, LNCS 5921, pages 402–417. Springer, Heidelberg (2009) ([196]).

- S. Mesnager. Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. IEEE Transactions on Information Theory-IT, Vol 57, No 11, pages 744–7458, 2011([199]).

- J-P Flori and S. Mesnager. Dickson polynomials, hyperelliptic curves and hyper-bent functions, Proceedings of the 7th International conference SEquences and Their Applications, SETA 2012, LNCS 7280, Springer, pages 40–52, 2012 ([102]).

Chapitre 3

Les fonctions booléennes sont utilisées dans de nombreux sytèmes de codage (leurs propriétés ont été étudiées en liaison avec la théorie des codes car elles sont étroitement liées aux propriétés des codes cycliques) et jouent un rôle central dans la sécurité des systèmes de chiffrements à flots ou par blocs (qui sont les deux grandes catégories de schémas de chiffrement à clef secréte). Elles interviennent comme éléments assurant la confusion de la fonction de chiffrement (concept défini par Shannon [233]).

Les fonctions booléennes utilisées dans les systèmes de chiffrement doivent donc vérifier plusieurs critères cryptographiques définis en réponse aux attaques inventées par les cryptanalystes.

Or, le cardinal de l'ensemble des fonctions booléennes étant doublement exponentiel en le nombre de variables, les critères cryptographiques ne peuvent pas être étudiés par simple investigation sur ordinateur, même pour des nombres de variables notoirement insuffisants. Des preuves mathématiques concernant les limites dans lesquelles les compromis peuvent être trouvés, et des constructions atteignant ces limites ou s'en approchant sont donc nécessaires. On ne peut en effet pas trouver des fonctions satisfaisant les critères cryptographiques à de bons niveaux par tirage aléatoire, les fonctions ayant les propriétés requises étant très peu denses dans l'ensemble de toutes les fonctions booléennes.

Au début du chapitre 3, nous rappelons les principaux critères que devrait vérifier une fonction booléenne pour un usage cryptographique. Le point important à noter est l'incompatibilité entre certains de ces critères (s'ils sont pris à des niveaux trop élevés) ce qui amène à en relâcher certains dans l'espoir de trouver des fonctions booléennes ayant de bonnes (à défaut d'optimales) propriétés cryptographiques (pour une description plus détaillée, le lecteur pourra consulter le Chapitre 8 de Claude Carlet [31]).

Synthèse des principaux résultats

1 – Profil de corrélation des fonctions booléennes. Dans un système de chiffrement à flots, il est important de générer les bits de chiffrement de manière à assurer le principe de confusion défini par Shannon. En effet, l'existence de corrélations entre la sortie de la fonction booléenne et certaines de ses entrées peut être exploitée pour mettre en œuvre une attaque de type "diviser pour régner" (voir *e.g.*[22, 251, 187, 236]). A cause de ce type d'attaque, il a été introduit les fonctions dites *sans corrélation* jusqu'à un certain ordre. Plus précisément, une fonction booléenne f est dite *sans corrélation d'ordre t* si sa distribution de valeurs ne change pas quand on fixe au plus t entrées. Le système de chiffrement est d'autant plus résistant aux attaques précédentes que la valeur de t est grande. Quand la fonction est sans corrélation d'ordre t et équilibrée, on dit alors que la fonction est t-résiliente.

Mais Siegenthaler [236] a montré que le degré algébrique d'une fonction sans corrélation d'ordre t est inférieur ou égal à $n-t$. De plus, il a été observé que la non-linéarité d'une fonction booléenne sans corrélation d'ordre t ne peut dépasser $2^{n-1} - 2^{\frac{n}{2}-1} - 2^t$ (quand n est pair) [46]. Quand la fonction est de plus équilibrée, les bornes supérieures sur le degré et la nonlinéarité des fonctions résilients d'ordre t sont plus basses. En effet, dans ce cas, le degré algébrique ne peut dépasser $n-t-1$ et la nonlinéarité est nécessairement inférieure ou égale à $2^{n-1} - 2^{t+1}$ si $\frac{n}{2} - 1 < t < n-1$ et $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{t+1}$ si $t \leq \frac{n}{2} - 1$ (n pair). Par conséquent, la propriété d'absence de corrélation à un ordre élevé n'est pas compatible avec la nécessité d'avoir un degré algebrique elevé (ce qui est requis à cause de l'attaque de Berlekamp-Massey et des attaques algébriques [72, 73, 226]) et une non-linéarité elevée (nécessaire à cause des attaques fondées sur les approximations affines des fonctions booléennes parmi lesquelles l'attaque par corrélation rapide). Il est donc impossible d'avoir une fonction booléenne sans corrélation avec un ordre elevé,

un haut degré algébrique et une haute nonlinéarité. Il est hélas classique en cryptographie de se retrouver face à une telle situation. Une attitude pourrait consister alors à se contenter d'une fonction ayant un ordre t d'immunité aux corrélations qui ne soit pas trop bas et ayant le plus haut degré possible et la meilleure non-linéarité possible. Une autre approche consiste à voir s'il est possible d'affaiblir certaines des trois conditions tout en ayant au final une fonction convenable pour un usage cryptographique. L'efficacité des attaques de Berlekamp-Massey et algébriques et des attaques linéaires font que la propriété qu'il semble le plus raisonnable d'affaiblir est la propriété d'absence de corrélation. Kurosawa et Matsumoto ([155]) avaient observé qu'il n'était pas nécessairement requis d'être sans corrélation avec un ordre élevé. En effet, ils ont observé que, pour les ordres élevés, la condition d'absence de corrélation entre entre la sortie de la fonction booléenne et certaines de ses entrées pouvait être relachée et qu'avoir des corrélations faibles semblait suffisant. Ils avaient alors proposé la notion de *quasi-résilience* fondée sur la distribution des sous-fonctions. Nous avons alors proposé une notion alternative à la quasi-résilience fondée elle sur la transformée de Walsh :

Définition 1. *Soit n un entier supérieur ou égal à 2. Soit φ une application définie sur $\{0,\ldots,n\}$ à valeurs dans $\mathbb{N}$. Une fonction booléenne sur $\mathbb{F}_2^n$ est dite avec φ-immunité aux corrélations si, pour tout, $\omega \in \mathbb{F}_2^n$,*

$$|\widehat{\chi_f}(\omega)| \leq \varphi(\mathrm{wt}(\omega))$$

où $\mathrm{wt}(\omega)$ désigne le poids de Hamming du mot ω. Lorsque, de plus, la fonction booléenne est équilibrée, elle est dite φ-résiliente.

La propriété définie ci-dessus est plus faible que l'absence de corrélation. Une fonction sans corrélation d'ordre t est en effet une fonction avec φ-immunité aux corrélations avec φ nulle sur $\{0,\ldots,t\}$. Nous nous sommes demandés si la notion de φ-corrélation entrait dans le cadre des travaux de Kurosawa et Matsumoto introduisant la quasi-résilience ([155]). Nous avons alors observé qu'aucune de ces deux notions ne recouvrait complètement l'autre. En revanche, nous avons montré plusieurs résultats reliant ces deux notions. En conclusion, chacune d'entre elles offre une notion alternative à l'absence de corrélation.

Évidemment, pour que la notion de φ-immunité aux corrélations soit intéressante, il est très important de restreindre le choix de φ. Nous avons alors analysé avec plus de finesse les attaques par corrélation [22, 251]. Le principe d'une attaque par corrélation est de se ramener à utiliser un algorithme de décodage d'un canal bruité. Il y a donc deux manières de rendre complexe ce type d'attaque : obliger à disposer d'une trop grande quantité d'information pour mettre en oeuvre l'attaque (complexité spatiale élevée) ou faire que l'algorithme de décodage ait une trop grande complexité temporelle. En considérant ces deux aspects, il a été montré qu'il fallait que $\varphi(l) = \mathcal{O}(\sqrt{l})$ pour être dans le premier cas alors qu'il suffisait que $\varphi(l) = \mathcal{O}(2^{\beta l})$ dans le second cas (profil de corrélation exponentiel). Nous avons ensuite considéré un autre type de système de chiffrement : les systèmes de chiffrement itérés, comme les systèmes de chiffrement auto-synchronisants. Nous avons montré qu'un tel système de chiffrement utilisant une fonction booléenne avec profil de corrélation exponentiel aurait ainsi une bonne résistance à l'attaque linéaire. Enfin, nous avons donné des constructions primaires et secondaires de fonctions booléennes avec profil de corrélation exponentiel.

2 – Sur le nombre de fonctions booléennes résilientes: Avoir une information sur le nombre de fonctions booléennes ayant une certaine propriété cryptographique particulière est très intéressant. Il permet par exemple de savoir si de telles fonctions sont rares ou fréquentes dans l'ensemble des fonctions booléennes. Mais généralement, compter les fonctions booléennes ayant une certaine propriété s'avère être un problème très difficile. Pour preuve, bien peu de résultats de ce type ont été trouvés jusqu'à nos jours.

Une famille de fonctions jouant un rôle important en cryptographie dont nous avons parlé dans le paragraphe précédent sont les fonctions dites résilientes. Beaucoup de travaux ont été menés sur ces fonctions. En revanche, on ne connait pas grand chose sur le nombre de fonctions booléennes m-résilientes à n variables, que nous noterons $\#Res_n^m$. En effet, on connait seulement le nombre de fonctions 1-résilientes pour $n \leq 7$ (le nombre de fonctions de fonctions 1-résilients en dimension 7 a été trouvé en 2007 [3]) et le nombre de fonctions m-résilientes lorsque $m \geq n-3$[17]. En dehors de ces résultats, les principaux résultats obtenus sont des bornes supérieures (Carlet et al. [37, 42]) et une estimation asymptotique (Canfield et al. [18]). En résumé, la valeur de $\#Res_n^m$ est donc inconnue. Pour tenter d'estimer ce cardinal, nous avons adopté une approche classique en combinatoire : écrire un cardinal au moyen d'une intégrale de Cauchy. Pour compter le nombre d'éléments d'un ensemble, il est courant en combinatoire d'interpréter ce cardinal comme un des coefficients d'une série génératrice. Dans cette optique, nous avons commencé par écrire le nombre de fonctions m-résilientes comme le cardinal d'un autre ensemble en s'appuyant sur la forme numérique normale des fonctions booléennes [38, 39].

Proposition 2. *Soit $\mathfrak{R}_n^m$ le sous-ensemble de $\mathbb{R}^{\Theta_n^m}$ défini par*

$$\mathfrak{R}_n^m = \Big\{ (x_J)_{J\in\Theta_n^m} \in \mathbb{R}^{\Theta_n^m} \;\Big|\; \forall I \in \mathcal{P}_n,\, 0 \leq \sum_{\substack{J\in\Theta_n^m \\ J\subset I}} x_J \leq 1 \Big\}. \tag{11.1}$$

Alors

$$\#Res_n^m = \#(\mathbb{Z}^{\Theta_n^m} \cap \mathfrak{R}_n^m).$$

Le résultat précédent ramène donc le problème de compter le nombre de fonctions m-résilientes à compter le nombre de points à coordonnées entières d'un polytope. L'étape suivante consiste alors à introduire une série génératrice à plusieurs variables et à exprimer le nombre de fonctions m-résilientes au moyen de l'intégrale de Cauchy d'une fraction rationnelle.

Proposition 3.

$$\#Res_n^m = \frac{1}{(2i\pi)^{2^n}} \oint G(z)\frac{dz}{z} \tag{11.2}$$

où G est définie par $z = (z_I)_{I\in\mathcal{P}_n}$ comme

$$G(z) = \prod_{I\in\mathcal{P}_n} (1+z_I) z_I^{-b_I-1} \cdot \prod_{J\in\Theta_n^m} \frac{1}{1-\prod_{\substack{I\in\mathcal{P}^n \\ J\subset I}} z_I}.$$

On peut en fait obtenir une autre représentation du même type pour $\#Res_n^m$ mais avec un polynôme à plusieurs variables à coefficients entiers.

Proposition 4.

$$\#Res_n^m = \frac{1}{(2i\pi)^{\#\Gamma_n^m}} \oint P(z) \prod_{I\in\Gamma_n^m} z_I^{-(b_I+1)} \frac{dz}{z}$$

où P est le polynôme à plusieurs indéterminées :

$$\forall z \in \mathbb{C}, \quad P(z) = \prod_{I\in\Gamma_n^m} (1+z_I) \prod_{J\in\Theta_n^m} \left(1 + \prod_{\substack{I\in\Gamma_n^m \\ J\subset I}} z_I^{a_{I,J}} \right)$$

avec

$$\forall (I,J) \in \Gamma_n^m \times \Theta_n^m, \quad a_{I,J} = \binom{\#I - \#J - 1}{n-m-\#J-1}.$$

Malheureusement, nous n'avons pas réussi jusqu'à présent à obtenir à partir de ces résultats de résultats concrets. Le grand nombre de variables rend difficile leur calcul. Néanmoins, elles offrent une nouvelle voie pour dénombrer les fonctions booléennes résilientes.

3 – Sur la non-linéarité d'ordre r des fonctions booléennes d'immunité algébraique donnée. Parmi les attaques apparues dans la littérature ces dernieres années, les attaques dites algébriques ont été l'objet de nombreux travaux. Pour quantifier la résistance à ces attaques algébriques d'un système de chiffrement par flot utilisant une fonction booléenne, un nouveau paramètre cryptographique à été introduit : l'*immunité algébrique*. L'immunité algébrique d'une fonction booléenne f est le plus petit degré d'un annulateur p de f ou $1+f$, i.e. vérifiant $fp = 0$ ou $(1+f)p = 0$. Un nouveau critère cryptographique a alors été défini : l'immunité algébrique d'une fonction booléenne utilisée dans un système de chiffrement par flot doit être la plus elevée possible (il a été montré que l'immunité algébrique d'une fonction booléenne à n variables était au plus égale à $\lceil \frac{n}{2} \rceil$).

Récemment, Carlet [30] a introduit une nouvelle notion : de *profil de non-linéarité* d'une fonction booléenne. Le profil de non-linéarité d'une fonction booléenne à n variables est la suite ordonnée des non-linéarités d'ordre r (où r varie de 1 à $n-1$) de la fonction booléenne, où la non-linéarité d'ordre r d'une fonction booléenne est définie comme la distance minimale de la fonction booléenne à l'ensemble des fonctions booléennes de degrés algébriques au plus r. Plusieurs travaux [72, 113, 137, 152, 204] ont montré l'importance d'étudier non seulement la non-linéarité d'ordre 1 mais aussi les non-linéarités d'ordre supérieures (i.e. la non-linéarité standard) en proposant d'autres approximations que les approximations affines (indiquons néanmoins que, pour être faisables, les attaques présentées dans ces travaux demandent une non-linéarité d'ordre r faible; signalons aussi que ce paramètre est aussi un indicateur important pour les systèmes de chiffrement par blocs).

Une question classique en cryptographie est d'étudier la compatibilité entre deux paramètres cryptographiques. Nous nous sommes alors intéressés à la non-linéarité d'ordre r des fonctions booléennes en relation avec leurs immunités algébriques. Nous nous demandions alors s'il était possible qu'une fonction ait à la fois un bon profil de nonlinéarité (valeurs élevées) et une haute immunité algébrique. Nous avons donc cherché à estimer la non-linéarité d'ordre r des fonctions booléennes ayant une immunité algébrique donnée.

Peu de résultats avaient été trouvés sur cette question. Principalement, il avait été montré par Lobanov en 2006 une borne inférieure sur la nonlinéarité d'ordre 1. Dans la même année, deux autres bornes inférieures sur la non-linéarité d'ordre r impliquant l'immunité algébrique ont été obtenues par Carlet et al. [34, 30] (mais aucune de ces deux bornes inférieures n'améliore l'autre dans tous les cas). En 2008, nous avons obtenu une nouvelle borne inférieure de la non-linéarité d'ordre r des fonctions Booléennes en fonction de leur immunité algébriques.

Théorème 5. *Soit f une variable à n-variables d'immunité algébrique k et soit r un entier positif strictement inférieur à k. Alors*

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$$

Cette nouvelle borne inférieure améliore de façon significative l'une des bornes inférieures proposées par Carlet et al. [34]pour tous les ordres tandis qu'elle n'améliore l'autre borne proposée par Carlet [30] que pour des ordres faibles (i.e. dans le cas le plus intéressant cryptographiquement). Pour obtenir cette borne inférieure sur la non-linéarité d'ordre r, nous avons commencé par minorer la distance entre une fonction booléenne f et une fonction booléenne g de degré algébrique

au plus r à l'aide de la dimension de l'espace des annulateurs d'une fonction h de degré au plus j, notée $d_{j,h}$.

Lemme 6. *Soit f une fonction à n variables vérifiant $AI(f) = k$. Soit r un entier positif strictement inférieur à k. Alors, pour toute fonction g à n variables de degré algébrique au plus r, we have*

$$\mathrm{dist}(f, g) \geq d_{k-1,g} + d_{k-1,1\oplus g}.$$

Puis, on utilise la minoration suivante sur ces dimensions $d_{k,g}$ à partir de laquelle nous avons déduit le théorème précédent.

Proposition 7. *Soit g une fonction booléenne à n variables de degré algébrique au plus r. Alors, pour tout entier positif k, $d_{k,g} \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$. Si g est le complément à un de l'indicatrice d'un sous-espace affine de $\mathbb{F}_2^n$ de dimension $(n-r)$ alors $d_{k,g} = \sum_{i=0}^{k-r} \binom{n-r}{i}$.*

Un point important est qu'à r fixé, cette borne inférieure ainsi que les résultats obtenus par Carlet et al. dépendent de manière croissante de $AI(f)$.

4 – Sur une conjecture combinatoire sur des mots binaires Comme nous l'avons indiqué dans le paragraphe précédent, l'apparition des attaques algébriques a rendu nécessaire pour un usage cryptographique qu'une fonction booléenne ait une immunité algébrique la plus haute possible. Plusieurs constructions de fonctions booléennes ayant une bonne immunité algébrique, mais pas nécessairement optimale, ont été proposées dans la littérature. Mais, très peu de fonctions ayant une haute immunité algébrique et vérifiant d'autres critères cryptographiques, comme être équilibrée ou avoir une haute non-linéarité, ont été trouvées. En fait, la plupart des fonctions booléennes proposées ayant une immunité algébrique optimale, i.e. telles qie $AI(f) = \lceil n/2 \rceil$, ont une nonlinéarité basse [49, 78, 164, 165, 51], souvent proche de la borne inférieure donnée par Lobanov [172]:

$$\mathrm{nl}(f) \geq 2^{n-1} - \binom{n}{\lfloor \frac{n}{2} \rfloor} .$$

En 2010, Tu et Deng [249] ont montré qu'il pouvait y avoir des fonctions booléennes de la classe des *Partial Spread*, introduite par Dillon [86], ayant une immunité algébrique optimale sous réserve que la conjecture suivante soit vraie.

Conjecture 8 (conjecture de Tu et Deng)**.** *Pour tout $k \geq 2$ et tout $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | a+b=t \text{ et } \mathrm{w_H}(a) + \mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

Tu et Deng ont vérifié par ordinateur que la propriété précédente était satisfaite pour $k \leq 29$. Ils ont aussi observé que, dans le cas où la conjecture est vérifiée, on pouvait obtenir en dimension paire des fonctions booléennes ayant une haute immunité algébrique et une haute non-linéarité (meilleure que celles des fonctions proposées par Carlet et Feng [50]).

Dans la poursuite des travaux de Tu et Deng, Tang et al. [246] ont utilisé une méthode récursive de construction de fonctions équilibrées avec haute non-linéarité, proposée par Dobbertin [94], pour construire à partir des fonctions de Tu et Deng [249, 248] des fonctions booléennes avec une meilleure non-linéarité.

Les fonctions obtenues par Tu et Deng semblaient prometteuses. Malheureusement, Carlet [47] observa qu'elles offraient une faible résistance aux attaques algébriques rapides. Carlet tenta sans succès de proposer une modification de la construction de Tu et Deng. Mais Wang et

Johansson [259] montrèrent qu'il serait difficile par des transformations simples de construire à partir des fonctions de Tu et Deng des fonctions résistantes aux attaques algébriques rapides.

En 2011, dans le même esprit que le travail de Tu et Deng [249], Tang, Carlet et Tang [245] proposèrent une famille infinie de fonctions booléennes ayant une bonne immunité algébrique avec une bonne résistance aux attaques algébriques rapides. Leur approche a principalement consisté à changer une division dans la construction de Tu et Deng en une multiplication. Néanmoins, comme Tu et Deng, ils avaient besoin pour montrer l'optimalité de l'immunité algebrique de leurs fonctions que soit vérifiée une famille d'inégalités :

Conjecture 9 (conjecture de Tang–Carlet–Tang)**.** *Pour tout $k \geq 2$ et tout $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid a-b=t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

Ils vérifièrent expérimentalement que l'inégalité précédente était vérifiée pour $k \leq 29$, ainsi que le résultat suivant, généralisant la conjecture précédente, pour $k \leq 15$.

Conjecture 10 (conjecture de Tang–Carlet–Tang)**.** *Soit $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ vérifiant $\gcd(u, 2^k-1) = 1$ et $\epsilon \in \{-1, 1\}$. Alors*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua+\epsilon b=t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

Cette dernière conjecture unifie la conjecture 9 et la conjecture de Tu et Deng (déduite en prenant $u = 1$ et $\epsilon = +1$). Les résultats de Tang, Carlet et Tang [245] furent repris et étendus par Jin et al. [139]. Dans leur article, leur principale idée est de remplacer y par y^{2^k-1-u} dans la construction de Tang, Carlet et Tang, ce qui permet d'unifier la famille de Tu et Deng [249], obtenue en posant $u = 1$, et la famille de Tang, Carlet et Tang [245], obtenue avec $u = 2^k - 2$. Comme les résultats de leurs prédécesseurs, ils ont du supposer que soit vérifiée une propriété:

Conjecture 11 (conjecture de Jin et al.)**.** *Soit $k \geq 2$ un entier, $t, u, v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ vérifiant $\gcd(u, 2^k-1) = \gcd(v, 2^k-1) = 1$. Alors*

$$\#\left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua+vb=t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1\right\} \leq 2^{k-1} \ .$$

En résumé, plusieurs conjectures ont été formulées qui sont vérifiées exclusivement expérimentalement par leurs auteurs. Leur principal intérêt réside dans le fait que de leur validité dépend de l'existence d'une fonction ayant une haute immunité algébrique avec une bonne non-linéarité.

Notons $S_{t,v,u,k}$ les ensembles qui interviennent dans les conjectures prédentes:

$$S_{t,v,u,k} = \left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \mid ua+vb=t; \mathrm{w_H}(a)+\mathrm{w_H}(b) \leq k-1\right\} \ ,$$

où $k \geq 2$, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ et $u, v \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^\times$, i.e. u et v admettent un inverse modulo 2^k-1. La conjecture de Tu et Deng postule que $\#S_{t,+1,1,k} \leq 2^{k-1}$ tandis que la conjecture de Tang, Carlet et Tang postule que $\#S_{t,-1,1,k} \leq 2^{k-1}$ ey $\#S_{t,\epsilon,u,k} \leq 2^{k-1}$. Enfin, la conjecture de Jin et al. dit que $\#S_{t,v,u,k} \leq 2^{k-1}$.

En 2010, nous avons entrepris l'étude de la conjecture de Tu et Deng [1]. Plus précisément, nous nous sommes intéressés à dénombrer les ensembles $S_{t,+1,1,k}$ (i.e. les ensembles de la conjecture de Tu et Deng). Pour cela nous avons introduit la fonction suivante[2] :

[1] En fait en 2010, seule la conjecture de Tu et Deng etait formulée. J-P. Flori [105] puis J-P. Flori et H. Randriam [106] ont poursuivi notre travail notamment dans plusieures directions et ont obtenu plusieurs résultats intéressants sur cette question.

[2] Cette fonction avait servi aussi dans les travaux de J-P. Flori et H. Randriam pour mieux comprendre les autres conjectures.

Définition 12. *Pour* $a, t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$,

$$r(a,t) = \mathrm{w_H}(a) + \mathrm{w_H}(t) - \mathrm{w_H}(a+t) \ ,$$

i.e. $r(a,t)$ *est le nombre de retenues générées par l'addition binaire de* a *et* t. *Et on pose*

$$r(0,t) = k \ ,$$

i.e. $r(0,t) = r(1,t)$. *La fonction* r *ainsi définie vérifie* $r(-t,t) = k$.

En utilisant la fonction r, nous avons alors reformulé la conjecture précédente en termes de "retenues" survenant dans une addition modulo $2^k - 1$. Ceci nous a permis d'une part de trouver des expressions explicites pour certains cardinaux $\#S_{t,+1,1,k}$ et d'autre part de montrer que la conjecture de Tu et Deng est vraie asymptotiquement. Nous avons également montré que la borne de la conjecture est atteinte pour certains entiers dont la representation binaire contient beaucoup de "1" et des "0" isolés. Nous conjecturons également que de tel entiers sont les seuls qui atteignent la limite. En outre, nous fournissons des informations qui n'ont malheureusement pas servis à fournir une preuve complète de la conjecture de Tu et Deng mais ont permis à Cohen et Flori de prouver que trés récemment que le cas particulier de la conjecture requis par la famille de Tang, Carlet et Tang [245] est vrai. Nos résultats ont contribué à une meilleure compréhension de ces conjectures qui sont de nature combinatoire. Malheureusement jusqu'a ce jour, la preuve complète de la conjecture Tu et Deng est toujours un problème ouvert malgré plusieurs tentatives et démonstrations fausses de certains chercheurs et une étude trés poussée réalisée par Flori et Randriambololona. De plus aucune conjecture presenté ci-dessus n'a été résolu sauf celle de Tang, Carlet et Tang dont la preuve de sa vilidité a été donnée trés récemment par G. Cohen et J.P Flori [67].

Publications

Les résultats présentés dans ce chapitre ont fait l'objet des publications suivantes :

- S. Mesnager. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. IEEE Transactions on Information Theory-IT, volume n°54 (8), pages 3656-3662, 2008 ([193]).
- S. Mesnager. On the number of resilient Boolean functions, Journal Number Theory and its Applications World Scientific, volume 5, pages 139-153, 2008 ([194]).
- C. Carlet, P. Guillot et S. Mesnager . On immunity profile of Boolean functions. Proceedings of 4-th International conference SEquences and Their Applications, SETA 2006. LNCS, pages 364-375, Springer, Heidelberg, 2006 ([40]).
- J-P. Flori, H. Randriambololona, G. Cohen et S. Mesnager. On a conjecture about binary strings distribution. Proceedings of 6-th International conference SEquences and Their Applications, SETA 2010, LNCS 6338, pages 346-358. Springer, Heidelberg, 2010 ([104]).

Chapitre 4

Les fonctions courbes forme une famille importante en théorie de l'information (cryptographie, codes correscteurs, sequences etc). Rothaus [227] les introduisit dans les années soixante et Dillon fut un des premiers à les étudier dans sa thèse [82]. Les fonctions courbes n'existent qu'en

dimension paire. En dimension $n = 2m$, les fonctions booléennes courbes sont les fonctions à distance $2^{n-1} - 2^{m-1}$ du code de Reed-Muller d'ordre 1, noté $\mathcal{RM}(1, n)$, c'est-à-dire l'ensemble des fonctions booléennes affines (de degré algébrique au plus 1). En fait, ce sont les fonctions à distance maximale de $\mathcal{RM}(1, n)$ et ce sont les seules qui possèdent cette propriété en dimension paire. Une manière[3] equivalente d'énoncer cette propriété est d'utiliser un paramètre important en cryptographie : la *non-linéarité*. La non-linéarité d'une fonction booléenne se définit alors comme la distance maximale de la fonction à l'ensemble des fonctions affines. En dimension paire, les fonctions courbes sont celle de non-linéarité maximale.

Un autre objet important associé à l'ensemble des fonctions courbes est, à dimension n fixée, ce qu'on appelle le groupe des automorphismes i.e. le groupe des permutations π de $\mathbb{F}_2^n$ telles que, pour toute fonction courbe f, la fonction $f \circ \pi$ est aussi courbe. Il a été montré que ce groupe coïncide avec le groupe général affine, c'est-à-dire le groupe des automorphismes linéaires, composé avec le groupe des translations par une fonction affine [31].

Cette propriété permet de définir une relation d'équivalence entre deux fonctions courbes appelée *EA-équivalence* : deux fonctions booléennes f et g sont dites EA-équivalentes s'il existe une fonction booléenne affine ℓ et un automorphisme affine A de $\mathbb{F}_2^n$ tels que $f = g \circ A + \ell$. Une classe de fonctions booléennes est alors dite *complète* si elle contient toutes les fonctions EA-équivalentes aux fonctions booléennes de la classe.

Il existe peu de classes infinies de fonctions courbes dans la littérature. La plus connue est la classe des fonctions courbes de Maiorana-McFarland. Une fonction $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ appartient à la classe de Maiorana-McFarland si elle s'écrit en représentation bivariée

$$\forall (x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m, \quad f(x, y) = \phi(x) \cdot y + g(y) \tag{11.3}$$

avec ϕ une permutation de $\mathbb{R}^m$ et g une fonction booléenne sur $\mathbb{R}^m$. Nous noterons dans la suite $\mathcal{M}$ la classe des fonctions courbes de Maiorana-McFarland et $\overline{\mathcal{M}}$ la classe complétée par EA-équivalence.

Dillon [82] introduisit dans sa thèse plusieurs autres classes infinies de fonctions courbes. Parmi ces classes, il a défini deux classes notées $\mathcal{PS}^-$ et $\mathcal{PS}^+$. Les fonctions booléennes de $\mathcal{PS}^-$ (resp. $\mathcal{PS}^+$) sont les fonctions booléennes dont les supports sont l'union de 2^{m-1} (resp. $2^{m-1}+1$) espaces vectoriels de dimension m deux à deux supplémentaires privés du vecteur nul et qui sont égales à 0 (resp. 1) en 0. La réunion de ces deux classes est notée $\mathcal{PS}$ et s'appelle dans la terminologie anglo-saxonne *Partial Spread class*.

Dillon a aussi introduit deux autres sous-familles de $\mathcal{PS}$: la classe $\mathcal{PS}_{ap}$, incluse dans $\mathcal{PS}^-$ et une famille qu'il a appelée "classe H". La famille $\mathcal{PS}_{ap}$ est l'ensemble des fonctions booléennes s'écrivant

$$\forall (x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m, \quad f(x, y) = g\left(yx^{2^m-2}\right) \tag{11.4}$$

en représentation bivariée où g est une fonction équilibrée nulle en 0. Pour définir la classe H, nous allons identifier $\mathbb{F}_2^n$ et $\mathbb{F}_{2^n}$ (qui est un espace vectoriel de dimension n sur $\mathbb{F}_2$). Une fonction booléenne n'est plus alors vue comme une fonction de $\mathbb{F}_2^n$ dans $\mathbb{F}_2$ mais comme une application de $\mathbb{F}_{2^n}$ dans $\mathbb{F}_2$ (qui est alors un sous-corps du corps $\mathbb{F}_{2^n}$; il existe plusieurs représentations des fonctions de $\mathbb{F}_{2^n}$ dans $\mathbb{F}_2$ que nous rappelons au Chapitre 1). La classe H est alors l'ensemble des fonctions de $\mathbb{F}_{2^n}$ dans $\mathbb{F}_2$ qui s'écrivent en représentation bivariée :

$$\forall (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}, \quad f(x, y) = \mathrm{Tr}_1^m(y + xG(yx^{2^m-2})) \tag{11.5}$$

où Tr_1^n désigne la trace d'un élément de $\mathbb{F}_{2^n}$ sur $\mathbb{F}_2$ et G est une permutation de $\mathbb{F}_{2^m}$ vérifiant

[3] Notez qu'il existe une autre manière de définir les fonctions courbes en termes de dérivées (i.e. dire que leur support est un ensemble différence)

(P1) $G(x) + x$ ne s'annule jamais

(P2) Pour tout $\beta \in \mathbb{F}_{2^m}^\star$, la fonction $G(x)+\beta x$ est 2-vers-1, c'est-à-dire, tout élément de l'ensemble d'arrivée à 0 ou 2 antécédents.

Enfin, récemment, de nouvelles familles de fonctions courbes ont été trouvées parmi les fonctions de Niho. Ces classes sont nouvelles en tant que représentations traces (si elles avaient été en représentation Forme Algébrique Normale alors on ne les aurait considérées comme nouvelles qu'après avoir montré qu'elles n'étaient pas déjà connues en tant que fonctions). Les fonctions de Niho sont les fonctions de $\mathbb{F}_{2^n}$ dans $\mathbb{F}_2$, $n = 2m$, dont les restrictions aux espaces vectoriels $\omega\mathbb{F}_{2^m}$ sont linéaires. Ces fonctions ont la particularité que leur représentation univariée est constituée exclusivement de monômes dont les exposants sont des entiers congrus à une puissance de 2 modulo $2^m - 1$.

Le concept de fonction courbe existe aussi pour les fonctions booléennes vectorielles, i.e. les fonctions de $\mathbb{F}_2^n$ dans $\mathbb{F}_2^r$. Nous appellerons de telles fonctions des (n, r)-fonctions.

Étant donnée une (n, r)-fonction F, les *fonctions coordonnées* de F sont les fonctions booléennes $f_1, \cdots, f_r$ définies par $F(x) = (f_1(x), \cdots, f_r(x))$ pour tout $x \in \mathbb{F}_2^n$. On appelle alors *fonction composante* de F toute combinaison linéaire des fonctions coordonnées à coefficients non tous nuls.

La *non-linéarité* d'une fonction vectorielle F est la non-linéarité minimale de ses fonctions composantes. Elle fut introduite par Nyberg [212] et, plus tard, étudiée par Chabaud et Vaudenay [53]. La non-linéarité d'une fonction vectorielle est un paramètre important en cryptographie car elle quantifie le niveau de résistance d'une boîte à substitution à l'attaque linéaire [181].

Les fonctions vectorielles courbes (aussi appelées fonctions parfaitement non-linéaires) sont les fonctions de non-linéarité maximale, c'est-à-dire, celles ayant la non-linéarité égale à $2^{n-1} - 2^{n/2-1}$. Un point important est que les (n, r)-fonctions courbes n'existent que quand n est pair et pour $r \leq n/2$ [211].

Cette contrainte fait que les fonctions vectorielles courbes ne sont pas utilisables seules pour concevoir une boîte à substitution, mais ces fonctions ont l'avantage d'offrir la meilleure résistance aux attaques différentielles et linéaires. Elles peuvent donc être utilisées pour construire des (n, n)-fonctions ayant une bonne résistance aux attaques linéaires et différentielles (voir [32]).

Synthèse des principaux résultats

1 – La classe $\mathcal{H}$. La condition (P1) donnée par Dillon pour définir la classe H n'est pas nécessaire pour assurer qu'une fonction de la forme (11.5) soit courbe. Elle sert en fait seulement à assurer que la classe H soit une extension de la classe $\mathcal{PS}$. La classe H de Dillon peut être vue comme un cas particulier d'une classe plus générale (que nous avons noté $\mathcal{H}$) dont les éléments sont des fonctions de $\mathbb{F}_{2^n}$ dans $\mathbb{F}_2$ dont la représentation bivariée est

$$g(x, y) = \mathrm{Tr}_1^m \left(\mu y (x^{2^m-1} + 1) + xG\left(y x^{2^m-2} \right) \right) \tag{11.6}$$

où G est une permutation de $\mathbb{F}_{2^m}$ vérifiant la propriété (P2) ci-dessus. Nous avons montré que la classe $\mathcal{H}$ coïncide avec la classe des fonctions courbes dont les restrictions aux espaces vectoriels $\omega\mathbb{F}_{2^m}$ sont linéaires, en d'autres termes, en représentation univariée, les éléments de la classe $\mathcal{H}$ sont les fonctions de Niho courbes. La classe $\mathcal{H}$ contient donc toutes les fonctions courbes trouvées dans [93, 160].

Cette nouvelle classe unifie donc plusieurs familles connues de fonctions courbes [82, 93, 160]. Elle offre par conséquent un cadre unique et général pour étudier les propriétés de ces familles. En particulier, nous avons utilisé ce cadre pour déterminer les duales de certaines des familles

présentées dans [93, 160] (voir le paragraphe 2). Autre apport important, nous avons montré qu'on pouvait associer les fonctions courbes de la classe $\mathcal{H}$ à une famille de polynômes étudiée en géométrie projective finie appelés les o-polynômes (voir le paragraphe 3). A la lumière de cette relation, nous avons proposé plusieurs familles de fonctions courbes potentiellement nouvelles grâce à la liste de o-polynômes établie par les géomètres pendant 40 ans. Pour l'instant, nous n'avons pas encore pu déterminer lesquelles de ces familles de fonctions courbes étaient réellement nouvelles (c'est-à-dire EA-inéquivalentes à une autre famille déjà connue).

Une extension naturelle, qu'on notera $\mathcal{K}$, de la classe $\mathcal{H}$ est de considérer les fonctions dont les restictions aux espaces $\omega\mathbb{F}_{2^m}^\star$ sont affines. Les fonctions de cette nouvelle classe sont les fonctions dont la représentation bivariée est

$$f(x,y) = \mathrm{Tr}_1^m\left(\mu y(x^{2^m-1}+1) + xG\left(yx^{2^m-2}\right) + F(yx^{2^m-2})\right) \tag{11.7}$$

où F est une application de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_{2^m}$. Si l'on prend $\mu = 0$ et $G = 0$ dans l'expression précédente, on obtient une fonction dont les restrictions aux espaces $\omega\mathbb{F}_{2^m}^\star$ sont constantes. En représentation univariée, les fonctions constantes sur $\omega\mathbb{F}_{2^m}^\star$ sont les fonctions booléennes dites *de Dillon*, c'est-à-dire les fonctions booléennes dont l'expression ne contient que des mônomes d' exposants congrus à 0 modulo $2^m - 1$ (les fonctions courbes de Dillon sont les fonctions de la forme $g(\delta x) + \mu$ avec $g \in \mathcal{PS}_{ap}$, $\delta \in \mathbb{F}_{2^n}^\star$ et $\mu \in \mathbb{F}_2$). Nous avons entièrement identifié les fonctions courbes dans cette nouvelle classe. En particulier, nous avons montré que la classe $\mathcal{K}$ englobe, en plus de celles de la classe $\mathcal{H}$ précédente, les fonctions de Dillon hyper-courbes (voir Chapitre 5).

Enfin, on signalera que la classe $\mathcal{K}$ contient aussi d'autres familles de fonctions booléennes sous-optimales mais intéressantes en cryptographie (Chapitre 8): des familles de fonctions booléennes semi-courbes en dimension paire.

2 – Les duales des fonctions courbes de la classe $\mathcal{H}$. La duale d'une fonction booléenne $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ est l'unique fonction booléenne $\tilde{f}$ définie par

$$\forall w \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(w) = (-1)^{\tilde{f}(w)} 2^m. \tag{11.8}$$

La duale $\tilde{f}$ d'une fonction booléenne courbe f possède la propriété remarquable d'être aussi une fonction booléenne courbe dont la duale est f.

Dobbertin et al [93] avaient laissé sans réponse la question suivante : les duales des fonctions de Niho courbes de [93] sont-elles EA-équivalentes à une des familles de [93] ? La classe $\mathcal{H}$ nous a permis d'avoir un nouveau regard sur les fonctions de [93]. Il est effet possible d'écrire la duale d'une fonction de la classe $\mathcal{H}$ comme la fonction caractéristique d'un certain ensemble.

Proposition 13. *Soit f une fonction booléenne de la classe $\mathcal{H}$ définie par (11.6). Alors la duale de f est la fonction caractéristique de l'ensemble*

$$\{(\alpha,\beta) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \in \mathbb{F}_{2^m} \mid G(z) + (\beta+\mu)z = \alpha \text{ n'a pas de solutions dans } \mathbb{F}_{2^m}\}. \tag{11.9}$$

Ce résultat ouvre une nouvelle voie pour le calcul des duales des fonctions de Niho courbes laissé en chantier dans [93, 160]. Pour deux des familles de [93, 160], nous avons réussi (dans un premier travail joint avec Carlet puis un second avec Budaghyan, Carlet, Helleseth et Kholosha) àà aller jusqu'au bout du calcul et à déterminer leurs duales.

Théorème 14. *Soit $n = 2m$ avec m impair et f définie par*

$$\forall t \in \mathbb{F}_{2^n}, \quad f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{(2^m-1)\frac{1}{4}+1})$$

où $a \in \mathbb{F}_{2^m}^\star$ et $b \in \mathbb{F}_{2^n}^\star$ vérifient $b^{2^m+1} = a$ et $b^4 \neq a^2$. Soit v défini par les relations $\mathrm{Tr}_m^n(v) = 1$ et $b^4 = a^2 v^{2^m-1}$. Alors, la duale de f est :

$$\widetilde{f}(a^{\frac{1}{2}}w) = \mathrm{Tr}_1^m\left(\left(v^{\frac{2^m+1}{2}} + 1 + \mathrm{Tr}_m^n(v^{2^m}w)\right)\left(\frac{\mathrm{Tr}_m^n(vw) + v^{\frac{2^m+1}{2}}}{\mathrm{Tr}_m^n(v^{-1})}\right)^{\frac{1}{3}}\right).$$

Et, le degré algébrique de la duale de f est $\frac{m+3}{2}$.

Théorème 15. *Soit $n = 2m$, $r > 1$ un entier vérifiant $\gcd(r, m) = 1$ et f une fonction booléenne sur $\mathbb{F}_{2^n}$ définie par*

$$f(t) = \mathrm{Tr}_1^n\left(at^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} t^{(2^m-1)\frac{i}{2^r}+1}\right),$$

avec $a \in \mathbb{F}_{2^n}$ vérifiant $a + a^{2^m} = 1$. Soit $u \in \mathbb{F}_{2^n}$ vérifiant $u + u^{2^m} = 1$. Alors la duale de f est égale à

$$\tilde{f}(w) = \mathrm{Tr}_1^m\left(\left(u(1 + w + w^{2^m}) + u^{2^{n-r}} + w^{2^m}\right)(1 + w + w^{2^m})^{1/(2^r-1)}\right).$$

De plus, le degré algébrique de $\tilde{f}(w)$ est égal à $d + 1$ où $d < m$ est l'unique entier positif vérifiant $dr \equiv 1 \pmod m$.

Le Théorème 14 répond notamment à la question posée précédemment car aucune des fonctions de [93] n'a un degré algébrique égal à $\frac{m+1}{3}$ pour $m > 3$; la fonction $\widetilde{f}$ du Théorème 14 est donc nécessairement EA-inéquivalente à toutes les fonctions introduites dans [93] (en effet, les degrés algébriques de fonctions EA-équivalentes sont nécessairement égaux).

3 – La classe $\mathcal{H}$ et les o-polynômes. Avant tout chose, rappelons que la propriété d'être courbe est conservée par l'addition d'une fonction linéaire. De plus, dire que G vérifie (P2) est équivalent à dire que $G + \nu$, $\nu \in \mathbb{F}_{2^m}$, vérifie (P2). Remarquons maintenant qu'en changeant G par $G + \mu$ et en additionnant à g la fonction linéaire $\mathrm{Tr}_1^m(\mu y)$ dans (11.6), on change g par $\mathrm{Tr}_1^m\left(xG\left(yx^{2^m-2}\right)\right)$. Nous pouvons donc supposer sans perte de généralité à partir de maintenant que $\mu = 0$.

Le fait important que nous avons observé est que la condition (P2) est équivalente à dire que,

(P3) Pour tout $\gamma \in \mathbb{F}_{2^m}$, l'application définie par

$$z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{si } z \neq 0 \\ 0 & \text{si } z = 0 \end{cases}$$

est une permutation de $\mathbb{F}_{2^m}$.

Or, les fonctions G vérifiant (P3) sont connues par les géomètres qui les appellent des o-polynômes et qui sont associés à des objets géométriques appelés dans la terminologie anglo-saxonne, *hyperovals*. Plusieurs familles (plus précisément 8 familles) de o-polynômes ont été trouvées dans la littérature pendant 40 ans :

1. $G(z) = z^6$ avec m impair [219];
2. $G(z) = z^{3\cdot 2^k+4}$, avec $m = 2k - 1$ [111];

3. $G(z) = z^{2^k+2^{2k}}$, avec $m = 4k-1$ [111];
4. $G(z) = z^{2^{2k+1}+2^{3k+1}}$, avec $m = 4k+1$ [111];
5. $G(z) = z^{2^k} + z^{2^k+2} + z^{3\cdot 2^k+4}$, avec $m = 2k-1$ [133];
6. $G(z) = z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}}$ avec m impair [221] (en notant que $G(z) = D_5\left(z^{\frac{1}{6}}\right)$, où D_5 est un polynôme de Dickson) [224];
7. $G(z) = \frac{\delta^2(z^4+z)+\delta^2(1+\delta+\delta^2)(z^3+z^2)}{z^4+\delta^2z^2+1} + z^{1/2}$, avec $\mathrm{Tr}_1^m(1/\delta) = 1$ et, si $m \equiv 2 \pmod 4$, alors $\delta \notin \mathbb{F}_4$ [262];
8. $G(z) = \frac{1}{\mathrm{Tr}_m^n(v)}\left[\mathrm{Tr}_m^n(v^r)(z+1) + \mathrm{Tr}_m^n\left[(vz+v^{2^m})^r\right]\left(z+\mathrm{Tr}_m^n(v)z^{1/2}+1\right)^{1-r}\right] + z^{1/2}$, avec m pair, $r = \pm\frac{2^m-1}{3}$, $v \in \mathbb{F}_{2^{2m}}$, $v^{2^m+1} = 1$ et $v \neq 1$ [263].

Chaque o-polynôme donné précédement permet d'obtenir une sous-famille de la classe $\mathcal{H}$. En fait, chacune des fonctions précédentes ne donne pas qu'une seule sous-famille de la classe $\mathcal{H}$. En effet, nous avons identifié plusieurs transformations possibles des o-polynômes ci-dessus donnant de nouvelles fonctions vérifiant (P2). La plupart de ces transformations conduisent à des fonctions booléennes courbes EA-équivalentes à celles déduites directement à partir de G. Nous avons identifié en revanche une transformation pouvant conduire à des fonctions EA-inéquivalentes. En effet, l'inverse d'un o-polynôme vérifie aussi la condition (P2) (en d'autres termes, l'inverse d'un o-polynôme est un o-polynôme). Dans certains cas, nous avons montré la EA-inéquivalence entre les o-polynômes de la classe $\mathcal{H}$ construites à partir de G et de G^{-1}.

1. m impair et $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{-5}y^6)$;
   - $f(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$.

   Les deux fonctions booléennes sont donc de même degré algébrique m. On ne peut donc rien conclure sur la EA-équivalence ou EA-inéquivalence de ces deux fonctions booléennes.
2. $m = 2k-1$ et $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$;
   - $f(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$.

   Le degré de la première fonction est égal à $m-1$ (si $k > 2$) et la seconde est de degré m (si $k > 2$). Par conséquent, ces deux fonctions sont EA-inéquivalentes.
3. $m = 4k-1$ et $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$;
   - $f(x,y) = \mathrm{Tr}_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$.

   Le degré des deux fonctions booléennes est égal à $3k$ nous ne pouvons donc rien conclure sur la EA-équivalence ou la EA-inéquivalence à partir du degré algébrique.
4. $m = 4k+1$ et $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^{2k+1}-2^{3k+1}}y^{2^{2k+1}+2^{3k+1}})$;

- $f(x,y) = \mathrm{Tr}_1^m(x^{2^{3k+1}-2^{2k+1}+2^k} y^{1-2^{3k+1}+2^{2k+1}-2^k})$

La première fonction booléenne est de degré $2k+1$ et la seconde de degré algébrique $3k+2$; les deux fonctions sont donc EA-inéquivalentes.

5. $m = 2k-1$ et $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{1-2^k} y^{2^k} + x^{-(2^k+1)} y^{2^k+2} + x^{-3\cdot(2^k+1)} y^{3\cdot 2^k+4})$;
   - $f(x,y) = \mathrm{Tr}_1^m\left(y\left(y^{2^k+1}x^{-(2^k+1)} + y^3 x^{-3} + yx^{-1}\right)^{2^{k-1}-1}\right)$..

   Les deux fonctions ont un degré algébrique m ce qui ne permet pas de conclure sur la EA-équivalence ou EA-inéquivalence de ces deux fonctions.

6. m impair et $x, y \in \mathbb{F}_{2^m}$:
   - $f(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}} y^{\frac{1}{6}} + x^{\frac{1}{2}} y^{\frac{1}{2}} + x^{\frac{1}{6}} y^{\frac{5}{6}})$;
   - $f(x,y) = \mathrm{Tr}_1^m\left(x\left[D_{\frac{1}{5}}\left(\frac{y}{x}\right)\right]^6\right)$ où $D_{\frac{1}{5}}$ est un polynôme de Dickson (1/5 désignant l'inverse de 5 modulo $2^{2m}-1$ (voir [224])

   La première fonction booléenne est de degré $\max(m,2,m) = m$. Nous laissons ouvert le problème qui consiste à déterminer une expression explicite de la seconde fonction ainsi que son degré.

Une question importante qui reste en suspens est de savoir si certaines des fonctions courbes précédentes n'appartiennent à aucune des classes connues de fonctions courbes, et notamment la classe de Maiorana-McFarland.

4 – Fonctions de Niho courbes et Subiaco / Adelaide hyperovales Grâce au cadre général offert par la classe $\mathcal{H}$, nous avons réussi à étendre une des familles introduites dans [93], i.e. les fonctions de la forme

$$f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{3(2^m-1)+1}) \tag{11.10}$$

avec $a \in \mathbb{F}_{2^m}^*$ et $b \in \mathbb{F}_{2^n}^*$. Les auteurs avaient montré dans [93] qu'une fonction booléenne de la forme (11.10) était courbe en supposant que $b^{2^m+1} = a$ et que b était la puissance cinquième d'un élément de $\mathbb{F}_{2^m}$. En écrivant les fonctions de cette famille sous la forme donnée par (11.7), i.e. en déterminant l'expression de la fonction G, nous avons observé avec Helleseth et Kholosha que la fonction G obtenue, dont l'expression dépend évidememnt de a et b, appartenait à une sous-famille connue de o-polynômes, les *Subiaco hyperovales* lorsque $b^{2^m+1} = a$. En d'autres termes, la deuxième condition introduite par les auteurs dans [93] n'est pas nécessaire (ce qui implique l'existence d'autres fonctions courbes qui n'étaient pas obtenues dans Dobbertin et al [93]) et les fonctions booléennes de la forme (11.10) sont donc courbes en supposant seulement que $b^{2^m+1} = a$.

Théorème 16. *Soit $n = 2m$, $b^{2^m+1} = a$ et $f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{3(2^m-1)+1})$*

1. *Supposons m impair. Soit $v = 1$ et $u \in \mathbb{F}_4 \setminus \{0,1\}$. Alors*

$$G(z) = a^{\frac{1}{2}} + \mathrm{Tr}_m^n(bu) + a^{\frac{1}{2}} f_s(z)$$

Si $b = 1$, alors

$$G(z) = \frac{z^2 + z}{(z^2 + z + 1)^2} + z^{1/2}$$

est un o-polynôme et donc f est courbe.

2. *Supposons $m \equiv 2 \pmod 4$. Soit $v = 1$, $u \in \mathbb{F}_{16} \setminus \mathbb{F}_4$ avec $u^5 = 1$ et $u + u^{2^m} = w$ où $w^2 + w + 1 = 0$. Alors*

$$G(z) = a^{\frac{1}{2}} + \mathrm{Tr}_m^n(b) + (1 + ws + s^{\frac{1}{2}})\,\mathrm{Tr}_m^n(b(u^4 + 1))f_s(z)$$

est un o-polynôme et donc $f(t)$ est courbe (aussi pour b qui n'est pas une puissance cinquième d'un élément de $\mathbb{F}_{2^n}$).

Signalons que la fonction G donnée dans le théorème précédent correspond au o-polynôme (g) dans la liste des o-polynômes du paragraphe précédent. En plus de ce résultat, nous avons aussi réussi (dans un travail commun avec Helleseth et Kholosha) àapporter une réponse à une question laissée ouverte concernant la fonction courbe suivante : $m = 4$, $f(t) = \mathrm{Tr}_1^m(t^{2^m+1}) + \mathrm{Tr}_1^n\left(t^{5(2^m-1)+1} + t^{7(2^m-1)+1}\right)$. Cette fonction avait été trouvée par Kholosha en 2004 suite à une recherche par ordinateur. A cette èpoque, Kholosha s'était demandé sans parvenir à répondre si cette fonction était vraiment nouvelle, i.e. si elle était EA-inéquivalente aux fonctions de Niho courbes connues. Nous avons répondu à son interrogation en montrant que cette fonction est EA-équivalente à une fonction booléenne courbe de la famille (11.10).

Enfin, nous avons montré également que la relation entre la classe des binomiales courbes de la forme $f(t) = \mathrm{Tr}_1^m(at^{2^m+1}) + \mathrm{Tr}_1^n(bt^{\frac{1}{6}(2^m-1)+1})$ ([93]) et les o-polynômes donne lieu à des *Adelaide hyperovales*.

A ce jour, tous les o-pôlynomes associés aux cinq familles de fonctions courbes connues de type Niho ont été identifié.

Pour conclure cette section, avec Carlet, nous avons introduit une nouvelle classe $\mathcal{H}$ de fonctions courbes qui est plus large que celle introduite par Dillon en 1974.

Les éléments de la classe $\mathcal{H}$ sont en représentation bivariée et constituent les fonctions courbes dont les restrictions aux espaces vectoriels (qui forment un spread) $\{E_a = \{(x, ax), x \in \mathbb{F}_{2^m}\}, a \in \mathbb{F}_{2^m}\}$ et $E_\infty = \{(0, y), y \in \mathbb{F}_{2^m}\}$ sont linéaires. En représentation univariée, les éléments de la classe $\mathcal{H}$ correspondent aux fonctions courbes de type Niho. Cette correspondance offre un nouveau cadre géneral pour étudier les propriétés des fonctions courbes de type Niho. Nous avons utilisé ce cadre pour répondre à plusieurs questions laissée ouvertes dans la littérature concernant les fonctions courbes connues de type Niho. Par ailleurs, nous avons établi un lien entre les éléments de la classe $\mathcal{H}$ (et donc les fonctions courbes de type Niho) et les o-polynômes qui sont des polynômes associés à des objets géométriques particuliers (du domaine de la géométrie projective finie). Ce lien nous a permis d'exploiter les travaux de recherche des géomètres (particulièrement difficiles !) des 40 dernières années et d'exhiber de nouvelles familles de fonctions courbes de type Niho (dont la liste etait relativement courte).

5 – Fonctions vectorielles courbes Construire des fonctions vectorielles courbes a motivé un certain nombre de travaux. On distingue généralement deux grands types de constructions de fonctions courbes: les constructions dites *primaires* qui sont des familles de fonctions courbes et les constructions dites *secondaires* dont le principe est de proposer un mécanisme de contruction de fonctions courbes à partir d'autres fonctions courbes.

A l'instar des fonctions booléennes, il existe des relations d'équivalence entre fonctions booléennes vectorielles. Pour les fonctions vectorielles booléennes, les relations d'équivalence les plus importantes sont l'EA-équivalence et la CCZ-équivalence. Deux (n,r)-fonctions F et F' sont dites EA-équivalentes s'il existe deux automorphismes affines L de $\mathbb{F}_2^n$ dans $\mathbb{F}_2^n$ et L' de $\mathbb{F}_2^r$ dans $\mathbb{F}_2^r$ et une fonction affine L'' de $\mathbb{F}_2^n$ dans $\mathbb{F}_2^r$ telles que $F' = L' \circ F \circ L + L''$. L'EA-équivalence est en fait un cas particuluer de la CCZ-équivalence [33]. Deux (n,r)-fonctions F et F' sont dites CCZ-équivalentes si leurs graphes $G_F := \{(x, F(x)),\ x \in \mathbb{F}_2^n\}$ et $G'_F := \{(x, F'(x)),\ x \in \mathbb{F}_2^n\}$ sont équivalents, au sens de l'équivalence affine, c'est-à-dire s'il existe une permutation affine $\mathcal{L}$ de $\mathbb{F}_2^n \times \mathbb{F}_2^r$ telle que $\mathcal{L}(G_F) = G'_F$.

Un point important est que la non-linéarité est invariante par CCZ-equivalence (et donc aussi par EA-équivalence). Récemment, Budaghyan et Carlet [12] ont montré que pour les fonctions vectorielles courbes et les fonctions booléennes à sortie simple, la CCZ-équivalence coïncide avec l'EA-équivalence.

Les constructions primaires de fonctions vectorielles courbes proviennent pour la plupart de constructions de fonctions booléennes adaptées aux fonctions vectorielles. Comme observé en premier par Nyberg dans [211], les deux principales familles de fonctions booléennes courbes peuvent être généralisées au cas des fonctions vectorielles conduisant à des grandes familles de fonctions vectorielles courbes. La première famille de fonctions vectorielles courbes est dans la lignée de la classe de *Maiorana-McFarland* et nous appelerons la classe de *Maiorana-McFarland* des fonctions vectorielles courbes. La deuxième famille est inspirée de la classe $\mathcal{PS}_{ap}$ introduite par Dillon. Les fonctions dans cette deuxième famille sont des fonctions vectorielles courbes dont les fonctions composantes appartiennent à la classe $\mathcal{PS}_{ap}$. Une troisième famille a été identifiée depuis : la classe de Maiorana-McFarland étendue.

Nous avons généralisé des constructions primaires connues et en avons proposé de nouvelles. En particulier, nous proposons une autre construction de fonctions vectorielles courbes dans l'esprit de la classe $\mathcal{PS}$. Nous avons ensuite étendu des constructions secondaires connues et proposé de nouvelles constructions secondaires de (n,r)-fonctions courbes.

Très récemment, nous avons montré que les o-polynômes permettent aussi la construction primaire de plusieures fonctions courbes vectorielles optimales :

Théorème 17. *Soit G un o-polynôme. Soient F, F' deux fonctions vectorielles de $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ à $\mathbb{F}_{2^m}$ tels que pour tout $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,*

$$F(x,y) = xG(yx^{2^m-2})$$

and

$$F'(x,y) = xG^{-1}(yx^{2^m-2})$$

Alors les fonctions F et F' sont courbes.

Publications

Les résultats présentés dans le chapitre 4 ont fait l'objet des publications suivantes :

- C. Carlet et S. Mesnager. On Dillon's class H of bent functions, Niho bent functions and o-polynomials. Journal of Combinatorial Theory-JCT-serie A 118, pages 2392–2410, 2011([44]).
- C. Carlet et S. Mesnager. On the construction of bent vectorial functions. Journal of Information and Coding Theory: Algebraic and Combinatorial Coding Theory, volume 1, No. 2, pages 133-148, 2010 [16].

- T. Helleseth, A. Kholosha et S. Mesnager. Niho Bent Functions and Subiaco/Adelaide Hyperovals. Proceedings of the 10-th International Conference on Finite Fields and Their Applications (Fq'10) Contemporary Math., AMS, 2012 ([126]).

- C. Carlet, T. Helleseth, A. Kholosha et S. Mesnager. On the Dual of Bent Functions with 2^r Niho Exponents. IEEE International Symposium on Information Theory, ISIT 2011, pages 703-707, Saint-Petersturg, Russie, 2011([41]).

- L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha et S. Mesnager. Further results on Niho bent functions. IEEE Transactions on Information Theory-IT. Vol. 58 no. 11, pages 6979–6985, 2012 ([14]).

Chapitre 5

Les fonctions hyper-courbes furent introduites par Youssef et Gong [271] à Eurocrypt en 2001. La première définition des fonctions hyper-courbes était fondée sur une propriété de la transformée de Hadamard, introduite par Golomb et Gong [115]. Les fonctions hyper-courbes présentent un intérêt à la fois théorique et pratique. En effet, d'une part, elles sont utlisées dans des boîtes à substitution; plus précisément, dans le système de chiffrement DES (The Data Encryption Standard). D'autre part, elles sont aussi intéressantes sur un plan théorique : elles sont en effet courbes mais surtout elles sont à distance maximale de l'ensemble des permutations monomiales de $\mathbb{F}_{2^n}$ (c'est-à-dire, des fonctions bijectives dont l'expression est la trace d'une puissance) et non seulement des fonctions affines comme les fonctions courbes. De telles fonctions sont certainement plus rares que les fonctions courbes et, d'ailleurs, à ce jour, on connait peu de familles de fonctions hyper-courbes. Même si elles doivent être moins nombreuses que les fonctions courbes, avoir une classification exhaustive des fonctions hyper-courbes semble illusoire et donc identifier le plus de familles de fonctions hyper-courbes est important et permettra certainement de mieux comprendre leur structure.

Comme indiqué dans [54], identifier des familles infinies de fonctions hyper-courbes est un problème difficile. En fait, depuis 2001, très peu de familles infinies de fonctions hyper-courbes ont été identifiées. La pluplart d'entre elles sont des fonctions monomiales courbes pour lesquelles on a simplement montré qu'elles sont aussi hyper-courbes (et la totalité de ces fonctions appartiennent à la classe $\mathcal{PS}_{ap}$). Récemment, Charpin et Gong [55, 54] ont considéré des fonctions sur $\mathbb{F}_{2^n}$ dont l'expression est de la forme $\sum_{r\in E} \mathrm{Tr}_1^n(\beta_r x^{r(2^m-1)})$, où E est un ensemble de représentants des classes cyclotomiques modulo 2^m+1 de taille maximale $n=2m$, et avec des coefficients β_r dans $\mathbb{F}_{2^n}$. Elles ont caractérisé au moyen des polynômes de Dickson et de sommes exponentielles les fonctions hyper-courbes potentielles de cette famille dans le cas où les coefficients β_r dans le sous-corps $\mathbb{F}_{2^m}$.Toutefois, il reste difficile d'expliciter à partir de leurs caractérisations des classes infinies de fonctions hyper-courbes, i.e. expliciter les coefficients β_r. Le résultat le plus abouti jusqu' à 2009 concernant les fonctions hyper-courbes dans l'esprit des travaux de [54] a concerné la fonction $\mathrm{Tr}_1^n(\beta x^{r(2^m-1)})$ où r est premier avec 2^m+1 pour laquelle il a été montré que cette dernière fonction est hyper-courbe si et seulement si β est un zéro d'une somme de Kloosterman [82],[54],[159]).

Synthèse des principaux résultats

Nous nous sommes intéressé aux deux familles de fonctions booléennes suivantes sur $\mathbb{F}_{2^n}$, $n=2m$ que nous avons introduites en 2009:

- la famille $\mathfrak{F}_n$ des fonctions booléennes de la forme :

$$f_{a,b}^{(r)}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}), \quad pgcd(r, 2^m+1) = 1$$

- la famille $\mathfrak{G}_n$ des fonctions booléennes de la forme

$$g_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

avec $a \in \mathbb{F}_{2^m}^\star$ et $b \in \mathbb{F}_4^\star$. Un premier point important est que, quand m est impair, ces deux familles sont des sous-familles d'une classe plus générale introduite par Dillon, la classe $\mathcal{PS}^-$. En effet, toutes les fonctions booléennes de ces deux familles possèdent la propriété d'être constantes sur les espaces $u\mathbb{F}_{2^m}^\star$ où u parcours le groupe cyclique U des racines (2^m+1)-ième de l'unité; les fonctions courbes de ces deux familles appartiennent donc à la classe $\mathcal{PS}^-$. Un second point important à noter est que les fonctions de ces deux familles appartiennent donc à l'extension $\mathcal{K}$ de la classe $\mathcal{H}$ introduite précédement (voir 11.7). Le troisième fait important est qu'aucune de ces deux familles ne rentre dans le cadre des travaux de Charpin et Gong [54]. Enfin, il n'existe pas dans ces deux familles d'autres fonctions courbes que celles qui sont hyper-courbes (en fait toutes les fonctions courbes de ces deux familles sont dans la classe de $\mathcal{PS}_{ap}^{\#}$).

Dans la lignée du résultat sur la fonction de Dillon $\mathrm{Tr}_1^n(\beta x^{2^m-1})$, nous avons réussi à identifier les fonctions hyper-courbes au moyen de sommes exponentielles quand m est impair :

Théorème 18. *Soit $n = 2m$ avec m impair ($m > 3$). Soit $a \in \mathbb{F}_{2^m}^\star$ et $b \in \mathbb{F}_4^\star$. Soit $f_{a,b}^{(r)}$ la fonction définie sur $\mathbb{F}_{2^n}$ par $f_{a,b}^{(r)}(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$ avec $pgcd(r, 2^m+1) = 1$*

1. *$f_{a,b}^{(r)}$ est hyper-courbe si et seulement si $K_m(a) = 4$.*
2. *$f_{a,b}^{(r)}$ est hyper-courbe si et seulement si $f_{a,b^2}^{(r)}$ est hyper-courbe.*
3. *Les fonctions courbes $f_{a,b}^{(r)}$ sont dans la $\mathcal{PS}_{ap}$ (resp. $\mathcal{PS}_{ap}^{\#}$) si $b = 1$ (resp. si $b \neq 1$).*
4. *La duale de la fonction courbe $f_{a,b}^{(r)}$ est $f_{a^{2^m},b^2}^{(r)}$.*

Dans la continuité de ce premier travail, nous avons poursuivi plus avant notre recherche théorique des éléments courbes de la famille $\mathfrak{F}_n$ dans le cas où m est pair tout en menant parallèlement une étude par ordinateur[4]. Nous avons montré que, pour toutes les fonctions courbes trouvées par ordinateur, la condition $K_m(a) = 4$ du théorème précédent est vérifiée. Ces résultats expérimentaux tentent à montrer que cette dernière condition serait nécessaire. Nous avons aussi expérimentalement déterminé les valeurs a pour lesquelles $K_m(a) = 4$ et regardé si les fonctions binomiales correspondantes étaient courbes. Nous avons observé que, pour toutes les valeurs de a trouvées, les fonctions binomiales courbes associées étaient en effet courbes. Ces résultats expérimentaux nous amènent à penser que la même condition que dans le cas impair serait une condition nécessaire et suffisante pour caractériser les éléments courbes de la famille $\mathfrak{F}_n$ dans le cas où m est pair. Néanmoins, nous n'avons pas réussi pour l'instant à confirmer théoriquement cette observation expérimentale.

[4] nous avons utilisé Sage [241] et Cython [9], les librairies Givaro [96], NTL [235] et gf2x [10] qui permettent de faire des calculs efficaces dans les corps finis

Nous avons ensuite étudié les fonctions de la famille $\mathfrak{G}_n$[5]. Nous avons montré que cette famille ne contenait aucune fonction courbe quand $m \equiv 3 \pmod 6$. En revanche, dans le cas où $m \not\equiv 3 \pmod 6$, nous avons identifié les fonctions courbes de $\mathfrak{G}_n$ au moyen de sommes exponentielles :

Théorème 19. *Soit $n = 2m$ avec m impair. Soit $a \in \mathbb{F}_{2^m}^\star$. Soit β un élément primitif de $\mathbb{F}_4$. Soit ζ un générateur du groupe cyclique U des racines (2^m+1)-ième de l'unité. Pour $(i,j) \in \{0,1,2\}^2$, soit $g_{a\zeta^i,\beta^j}$ une fonction booléenne appartenant à la famille $\mathfrak{G}_n$*

1. *Supposons $m \not\equiv 3 \pmod 6$. Alors:*

   - *Si $\mathrm{Tr}_1^m(a^{1/3}) = 0$ alors, pour tout $(i,j) \in \{0,1,2\}^2$, la fonction $g_{a\zeta^i,\beta^j}$ est (hyper)-courbe si et seulement si $K_m(a) = 4$.*

   - *Si $\mathrm{Tr}_1^m(a^{1/3}) = 1$ alors:*

     (a) g_{a,β^j} n'est pas courbe pour tout $j \in \{0,1,2\}$.

     (b) Pour tout $i \in \{1,2\}$, $g_{a\zeta^i,\beta^j}$ est (hyper)-courbe si et seulement si $K_m(a) + C_m(a,a) = 4$.

2. *Supposons $m \equiv 3 \pmod 6$. Alors, pour tout $i \in \{0,1,2\}$, $g_{a\zeta^i,b}$ n'est pas courbe pour toute valeur de $a \in \mathbb{F}_{2^m}^\star$ et $b \in \mathbb{F}_4^\star$.*

La duale d'une fonction courbe $g_{a,b}$ de $\mathfrak{G}_n$ appartient à $\mathfrak{G}_n$ et est égal à $g_{a^{2^m},b^2}$

En conclusion, nous avons réussi à identifier toutes les fonctions (hyper)-courbes de ces deux familles au moyen de sommes exponentielles classiques : sommes de Kloosterman et sommes cubiques.

Publications

Les résultats présentés dans le chapitre 5 ont fait l'objet des publications suivantes :

- S. Mesnager. A new family of hyper-bent Boolean functions in polynomial form. Proceedings of Twelfth International Conference on Cryptography and Coding. Cirencester, United Kingdom. M. G. Parker (Ed.) IMACC 2009, LNCS 5921, pages 402–417. Springer, Heidelberg (2009) ([196]).

- S. Mesnager. A new class of Bent Boolean functions in polynomial forms. Proceedings of international Workshop on Coding and Cryptography, WCC 2009, pages 5-18, Ullensvang, Norway, pages 5–18, 2009([195]).

- S. Mesnager. A New Class of Bent and Hyper-Bent Boolean Functions in Polynomial Forms. Journal Designs, Codes and Cryptography (DCC) volume 59, Numbers 1-3, pages 265-279, 2011([197]).

[5]Notez que la partie monomiale des fonctions de la classe $\mathfrak{G}_n$ i.e. $\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right)$ n'est jamais courbe car l'exposant $3(2^m-1)$ n'est pas un exposant courbe puisqu'il ne verifie pas les conditions nécessaires pour qu'un exposant monomial soit courbe. En revanche, la partie monomiale de la classe $\mathfrak{F}_n$ i.e. $\mathrm{Tr}_1^n(ax^{r(2^m-1)})$ est courbe si et seulement si a est un zéro de la somme de Kloosterman definie sur $\mathbb{F}_{2^m}$

Chapitre 6

Charpin et Gong se sont attaquées dans [54] à extraire les fonctions courbes définies sur $\mathbb{F}_{2^n}$ de la forme

$$\sum_{r\in R} \mathrm{Tr}_1^n(\beta_r x^{r(2^m-1)})$$

où $n := 2m$ et R est un ensemble de représentants des classes cyclotomiques modulo 2^m+1 de taille maximale $n = 2m$ et $\beta_r \in \mathbb{F}_{2^n}$.

Quand r est premier avec 2^m+1, on remarque que l' exposant de chacun des termes dans l'expression des fonctions précédentes est un exposant de Dillon. L'ensemble des fonctions courbes et hyper-courbes de la forme précédente coïncide donc.

Pour identifier les fonctions hyper-courbes de la forme précédente, Charpin et Gong se sont restreintes au cas où tous les coefficients β_r appartenaient à $\mathbb{F}_{2^m}$. Et avec cette restriction, elles ont introduit dans [54] des caractérisations très intéressantes du carractère courbe des fonctions de la forme ci-dessus en utilisant les polynômes de Dickson.

Synthèse des principaux résultats

Dans la continuité des resultats de Charpin et Gong, nous avons cherché à obtenir des caractérisations similaires aux leurs pour les éléments d'une sous-famille $\mathfrak{H}_n$ de PS^-. Cette sous-famille $\mathfrak{H}_n$ est constituée des fonctions booléennes de la forme

$$\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$$

où R est un ensemble de représentants des classes cyclotomiques modulo 2^n-1 de taille maximale $n := 2m$, $\{a_r,\, r \in R\}$ est un sous-ensemble de $\mathbb{F}_{2^m}$ et b est un élément de $\mathbb{F}_4^\star$.

Cette famille $\mathfrak{H}_n$ contient en particulier les familles $\mathfrak{F}_n$ et $\mathfrak{G}_n$ éudiées dans le chapitre précédent. Nous avons alors caractérisé les éléments (hyper)-courbes de cette famille au moyen de sommes exponentielles et de polynômes de Dikcon de degré r et 3. En particulier, quand b est un élément primitif de $\mathbb{F}_4$, nous avons ramené la question de savoir si un élément de $\mathfrak{H}_n$ est (hyper)-courbe ou non au calcul du poids de Hamming d'une certaine fonction booléenne.

Théorème 20. *([192]) Soit $n = 2m$ avec m impair. Soit $b \in \mathbb{F}_4^\star$ et β u élément primitif de $\mathbb{F}_4$. Soit $f_{a_r,b}$ une fonction de la famille $\mathfrak{H}_n$. Soit g_{a_r} la fonction booléenne définie sur $\mathbb{F}_{2^m}$ par $g_{a_r}(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x))$, où $D_r(x)$ est le polynôme de Dockson de degré r.*

1. *$f_{a_r,b}$ est hyper-courbe si et seulement si $f_{a_r,b}$ est courbe.*
2. *Les fonctions courbes $f_{a_r,b}$ appartiennent à la classe $\mathcal{PS}^-$. De plus, les fonctions courbes $f_{a_r,b}$ sont dans la classe $\mathcal{PS}_{ap}$ (resp. $\mathcal{PS}_{ap}^{\#}$) si $b = 1$ (resp. si $b \neq 1$).*
3. *Les trois énoncés suivants sont alors équivalents :*
   - *(a) $f_{a_r,\beta}$ est hyper-courbe;*
   - *(b) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star, \mathrm{Tr}_1^m(x^{-1})=1} \chi\Big(g_{a_r}(D_3(x))\Big) = -2$;*
   - *(c) $\displaystyle\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(\mathrm{Tr}_1^m(x^{-1}) + g_{a_r}(D_3(x))\Big) = 2^m - 2\,\mathrm{wt}(g_{a_r}\circ D_3) + 4.$*

4. $f_{a_r,1}$ *est hyper-courbe si et seulement si,*
$2\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g_{a_r}(D_3(x))\Big)-3\sum_{x\in\mathbb{F}_{2^m}^\star,\mathrm{Tr}_1^m(x^{-1})=1}\chi\Big(g_{a_r}(x)\Big)=2.$

Dans le chapitre précédent, nous avions ramené le problème d'identifier les éléments hyper-courbes de la famille $\mathfrak{F}_n$ à déterminer les valeurs de $\mathbb{F}_{2^m}$ pour lesquelles la somme de Kloosterman $K_m(a)$ prenait la valeur 4. Les caractérisations obtenues ici sont aussi des sommes exponentielles mais moins explicites que celles obtenues dans le chapitre précédent (où les fonctions considérées étaient des binomiales). Mais, néanmoins, on peut montrer qu'on retrouve à partir des caractérisations présentées dans le théorème précédent tous les résultats présentés dans le chapitre précédent pour les familles $\mathfrak{F}_n$ et $\mathfrak{G}_n$.

En reprenant notre approche, Wang, Tang, Qi, Yang et Xu [258] ont considéré la famille suivante (en remplaçant le terme sur $\mathbb{F}_4$ par un terme sur $\mathbb{F}_{16}$) :

$$f_{a,b}(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)+\mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$$

où les coefficients a_r sont dans $\mathbb{F}_{2^m}$, le coefficient b est dans $\mathbb{F}_{16}$ et m est choisi tel que $m\equiv 2 \pmod 4$. L'ensemble R est le même que le nôtre.

En collaboration avec Flori, nous avons raffiné les résultats de Wang et *al.* en ajoutant les expressions de leurs transformées de Walsh, leurs degrés algébriques et leurs duales.

Dans le but d'apporter un point final à ce type de question, nous avons entrepris l'étude de la famille des fonctions booléennes de la forme générale :

$$f_{a,b}(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)+\mathrm{Tr}_1^t\left(bx^{s(2^m-1)}\right)$$

où $n=2m$ est une entier pair, R est un ensemble de représentants des classes cyclotomiques modulo 2^m+1, les coefficients a_r sont dans $\mathbb{F}_{2^m}$, s est un diviseur de 2^m+1, i.e. $s(2^m-1)$ est un exposant de Dillon, $t=o(s(2^m-1))$, i.e. t est la taille de la classe cyclotomique de s modulo 2^m+1, le coefficient b est dans $\mathbb{F}_{2^t}$.

Cette dernière classe recouvre l'ensemble des familles précédentes (y compris celle de Wang, Tang, Qi, Yang et Xu [258]) ainsi que d'autres qui sont encore non étudiées.

Nous avons cherché à caractériser de la manière la plus simple possible les fonctions hyper-courbes de la forme précédente. Nous avons réussi à les écrire aussi à l'aide de sommes exponentielles et de polynômes de Dickson. Malheureusement, nous avons obtenu des caractérisations plus complexes que dans les cas précédents et difficilement exploitables dans l'immédiat pour expliciter des familles concrètes de fonctions hyper-courbes.

Publications

Les résultats présentés dans le chapitre 6 ont fait l'objet des publications suivantes :

- S. Mesnager. Hyper-bent Boolean Functions with Multiple Trace Terms. Proceedings of International Workshop on the Arithmetic of Finite Fields. WAIFI 2010, LNCS 6087, pages. 97–113. Springer, Heidelberg, 2010 ([192]).
- S. Mesnager Bent and Hyper-bent Functions in polynomial form and Their Link With Some Exponential Sums and Dickson Polynomials. IEEE Transactions on Information Theory-IT, Vol 57, No 9, pages 5996-6009, 2011 ([198]).
- S. Mesnager et J.P Flori. On hyper-bent functions via Dillon-like exponents. IEEE International Symopsium on Infomation Theory ISIT 2012. IMT, Cambridge, MA, USA, 2012 ([202])

Chapitre 7

Un lien entre sommes exponentielles et variétés algébriques avait été mis en lumière il y longtemps, permettant de transférer l'étude de sommes exponentielles à l'étude de variétés algébriques. Ce lien a été exploité par plusieurs auteurs : Weil [264] qui a déduit de l'hypothèse de Riemman une borne pour les sommes de Kloosterman; Leonard et Williams [161] ont exprimé des sommes de Kloosterman au moyen de courbes elliptiques; Lachaud et Wolfmann [157], et Katz et Livné [146], exploitèrent la théorie des courbes elliptiques pour étudier la distribution de sommes de Kloosterman.

Très récemment Lisonek [170] a utilisé ce lien pour réécrire la caractérisation de Charpin et Gong [54] et ramener la vérification de la condition énoncée par cette caractérisation à compter les points de courbes hyperelliptiques. Il en a alors déduit (grâce un algorithme de comptage de points sur une courbe hyperelliptique) un algorithme pour identifier les éléments hyper-courbes d'une sous-famille de la famille considérée par Charpin et Gong.

Synthèse des principaux résultats

Dans le chapitre 7, nous reprenons l'approche de Lisonek[6] mais dans un cadre plus général et en reformulant de manière générique le lien entre des sommes exponentielles (qui interviennent dans les critères de (hyper)-courbes) et des cardinaux de courbes hyperelliptiques. Plus précisément nous avons établie les deux propositions suivantes:

Proposition 11.0.1. *Soit $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ une fonction telle que $f(0) = 0$, $g = \mathrm{Tr}_1^m(f)$, et G_f la courbe (affine) définie sur $\mathbb{F}_{2^m}$ par*

$$G_f : y^2 + y = f(x) \ .$$

Alors

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) = -2^m - 1 + \#G_f \ .$$

Proposition 11.0.2. *Soit $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ une fonction , $g = \mathrm{Tr}_1^m(f)$, et H_f la courbe (affine) définie sur $\mathbb{F}_{2^m}$ par*

$$H_f : y^2 + xy = x + x^2 f(x) \ ,$$

Alors

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(\mathrm{Tr}_1^m(1/x) + g(x)) = -2^m + \#H_f \ .$$

Dans un travail conjoint avec Flori, nous avons alors reformulé les caractérisations proposées par Wang et al. et les nôtres (présentées dans le chapitre précédent) au moyen de cardinaux de courbes hyperelliptiques. Nous avons présenté ensuite un algorithme permettant de tester si un élément de la famille $\mathfrak{H}_n$ (resp. de la famille de Wang et al.) est hyper-courbe ou non. Néanmoins, l'algorithme obtenu n'offre pas un moyen trés efficace d'identifier explicitement les fonctions hyper-courbes de $\mathfrak{H}_n$. Dans ce but, nous avons présenté un raffinement de cet algorithme afin d'obtenir un test plus efficace, plus rapide en pratique, pour vérifier si un élément de $\mathfrak{H}_n$ est hyper-courbe ou non. Nous avons en effet montré que la complexité temporelle et spatiale de l'

[6] Dans l'ordre chronologique de nos résultats, nous avons en fait repris l'esprit de la démarche de Lisonek pour la première fois dans le cadre des fonctions semi-courbes

algorithme ainsi obtenu est polynomiale pour certaines sous-familles de $\mathfrak{H}_n$. L'idée du raffinement de l'algorithme consisté à uliliser des propriétes mathématiques de certaines applications faisant intervenir les polynômes de Dickson. Ceci a permis d'éviter de calculer certains cardinaux de courbes hyperelliptiques.

L'apport fondamental et principal, comme l'ont montré nos résultats numériques, est que les caractérisations utilisant les courbes hyperelliptiques fournissent un moyen plus efficace, et pas seulement asymptotiquement, pour identifier les fonctions hyper-courbes que les caractérisations utilisant des sommes exponentielles.

Dans la dernière partie du Chapitre 7, nous rappelons des résultats classiques sur la divisibilité des sommes de Kloosterman binaires et donnons d'autres preuves de ces résultats utilisant la théorie des courbes elliptiques. Nous proposons différentes stratégies pour trouver les zéros des sommes de Kloosterman binaires et développons un algorithme pour déterminer en quels points une somme de Kloosterman binaire prend la valeur 4.

Publications

Les résultats présentés dans le Chapitre 7 ont fait l'objet des publications suivantes :

- J.P. Flori et S. Mesnager. Dickson polynomials, hyperelliptic curves and hyper-bent functions. Proceedings of 7-th International conference SEquences and Their Applications, SETA 2012, LNCS 7280 , pages 40–52. Springer, Heidelberg, 2012 ([102]).

- J.P. Flori, S. Mesnager et G. Cohen. Binary Kloosterman sums with value 4. Proceedings of Thirteenth International Conference on Cryptography and Coding, IMACC 2011, LNCS 7089, pages 61-78, Springer, 2011([103]).

Chapitre 8

De nombreux travaux ont été consacrés à la résistance de systèmes de chiffrement aux attaques par corrélation rapides (pour les systèmes de chiffrement par flot) ou aux attaques linéaires (pour les systèmes de chiffrement par blocs). Notamment, différents raffinements de ces attaques ont été étudiés et plusieurs constructions de fonctions booléennes offrant une bonne résistance à ces attaques ont été proposées. Parmi ces constructions, une famille joue un rôle central : les fonctions courbes [227] (dont nous avons beaucoup parlé dans le Chapitre 4). D'autres familles jouent aussi un rôle important à savoir la sous-famille des fonctions courbes homogènes [223] et les fonctions hyper-courbes [271], les fonctions Z-courbes[92] et negabent [218].

Un des traits importants des fonctions courbes est qu'elles ne sont pas équilibrées, ce défaut fait qu'il n'est pas possible de les utiliser directement pour concevoir un système de chiffrement. Or il existe une autre famille de fonctions booléeennes dont la non-linéarité est haute : la famille des fonctions *semi-courbes* [62]. L'intérêt de ces fonctions est que le spectre de Walsh contient la valeur 0 et donc que la fonction peut être équilibrée simplement par l'addition d'une fonction affine (la fonction ainsi obtenue a exactement la même non-linéarité que la fonction de départ). Cette famille a été introduite par Chee, Lee et Kim à Asiacrypt en 1994 [62]. Elles ont été tout d'abord présentées comme les seules fonctions dont le spectre de Walsh est de cardinal 3 et ayant la plus haute non-linéarité [19]. Cette famille est en fait une sous-famille de la famille des fonctions dites *plateaux* [276, 275]. Elles sont étudiées car, à l'instar des fonctions courbes, leurs transformées de Walsh ne prennent pas de grandes valeurs, propriété importante à cause de l'attaque par corrélation rapide [188] et l'attaque linéaire [182]. Certaines d'entre elles possèdent une immunité aux corrélations, vérifient les critères de propagation pour des ordres élevés et

ont une fonction d'autocorrélation prenant de petites valeurs. En revanche, elles partagent avec les fonctions courbes le défaut de ne pas pouvoir être de degré algébrique élevé (au plus $n/2$ en dimension n paire; mais, comme les fonctions courbes, elles peuvent être utilisées pour construire des fonctions booléennes avec de bonnes propriétés cryptographiques [31]). Plusieurs familles différentes de fonctions semi-courbes en dimension paire ont été proprosées dans la littérature : fonctions partiellement courbes [31] de noyau de dimension 2, restrictions à un sous-espace $\{a, b\}^{\perp}$ de co-dimension 2 de fonctions courbes dont les dérivées secondes $D_a D_b \widetilde{f}$ de la duale de la fonction courbe est nulle [19, 20].

Dans [59], Charpin et al. donnent une condition nécessaire et suffisante pour qu'une fonction booléenne quadratique booléenne soit semi-courbe. D'autres constructions sont aussi proposées dans [62, 242]; mais, les fonctions ainsi obtenues représentent probablement une très faible partie de l'ensemble des fonctions semi-courbes.

Les fonctions semi-courbes existent en dimension paire et aussi en dimension impaire. Quand n est pair, le spectre des Walsh des fonctions semi-courbes est constitué des trois valeurs 0 et $\pm 2^{\frac{n+2}{2}}$. Elles peuvent être équilibrées par addition d'une fonction linéaire et ont la non-linéarité maximale qu'une fonction plateau peut avoir. Quand n est impair, on ne connait pas la non-linéarité maximale d'une fonction plateau. En revanche, on connait la non-linéarité maximale des fonctions quadratiques, qui sont toutes des fonctions plateaux, qui est égale à $2^{n-1} - 2^{\frac{n-1}{2}}$ [176] (en petite dimension, il a été observé que cette valeur était aussi la non-linéarité maximale d'une fonction plateau [209]). Les fonctions qui atteignent la borne précédente sont appelées semi-courbes en dimension impaire. Leurs spectres de Walsh sont constitués des trois valeurs 0, $\pm 2^{\frac{n+1}{2}}$ [63].

Plusieurs auteurs de la communauté de la théorie des séquences se sont intéressés à trouver des familles de fonctions semi-courbes. En effet, les fonctions de haute non-linéarité correspondent aux séquences faiblement corrélées avec les m-séquences (les séquences de longueur maximale générée par les registres linéaires à décalage) [127] [125].

Les principales constructions de fonctions semi-courbes sont dues à Gold [112], Niho [210], Helleseth [124, 125], Helleseth et Kumar [127]. Toutefois, la plupart des familles proposées dans ces travaux sont construites à partir de fonctions puissances, i.e. les fonctions de la forme $x \mapsto \mathrm{Tr}_1^n\left(x^d\right)$, en dimension impaire. Khoo, Gong et Stinson [149] ont trouvé une nouvelle famille de séquences semi-courbes et ont obtenu dans [150] des fonctions semi-courbes quadratiques en dimension impaire (plus précisement des combinaisons linéaires de fonctions de Gold). Leurs résultats ont été étendus par Charpin, Pasalic et Tavernier [59] à d'autres familles de fonctions quadratiques. En particulier, ces derniers ont montré comment obtenir une fonction semi-courbe cubique par concaténation de fonctions courbes quadratiques.

Synthèse des principaux résultats

A l'instar de nos travaux sur les fonctions hyper-courbes, notre motivation a été de caractériser les fonctions semi-courbes de plusieurs familles de fonctions booléennes à l'aide de sommes exponentielles en dimension paire et par suite proposer des nouvelles constructions. Dans un premier travail, nous avons considéré des fonctions booléennes en forme univariée et dont chaque terme est une fonction monôme dont l'exposant est de Dillon ou de Niho [201]. De plus, nous avons également fourni des caractérisations efficaces du caractère "semi-courbe" pour plusieurs familles de fonctions en termes de cardinaux de courbes hyperelliptiques. Ce travail fut en fait notre premier travail[7] dans l'esprit des résultats de Lisonek.

[7]Dans l'ordre chronologique, nous avons établis ces résultats avant ceux concernant la propriété "hyper-courbe". Plus précisément, nous avons utilisé l'idée de l'approche de Lisonek dans le cadre des fonctions semi-courbes avant de l'étendre au cadre des fonctions hyper-courbes.

Notre etude sur les constructions explicites de familles infinies de semi-courbes nous a permis de penser que les fonctions semi-courbes dont la restriction aux espaces $u\mathbb{F}_{2^m}^\star$ où u parcours le groupe cyclique des racines 2^m+1-ème de l'unité, sont essentiellement les fonctions obtenues en additionnant une fonction courbe de type Niho et une fonction de la classe $\mathcal{PS}_{ap}^{\#}$. Dans un travail avec C. Carlet nous avons alors généralisé les constructions de fonctions semi-courbes que nous avons proposées dans [199] puisque nous avons montré dans [45] comment construire des fonctions semi-courbes en dimension paire à partir de fonctions de $\mathcal{PS}_{ap}$ et une fonction courbe dont les restrictions à certains sous-espaces vectoriels, formant ce qu'on appelle dans la terminologie anglo-saxonne un *spread*, sont linéaires.

Théorème 21. *Soit $m \geq 2$ avec $n = 2m$. Soit $\{E_i,\, i = 1, \ldots, 2^m+1\}$ des sous-espaces-vectoriels de $\mathbb{F}_{2^n}$ et h une fonction booléenne dont la restriction à chacun des sous-espaces vectoriels E_i est linéaire (éventuellement nulle). Soit S un sous-ensemble de $\{1, \ldots, 2^m+1\}$. Posons $g = \sum_{i\in S} 1_{E_i}$ (mod 2) où 1_{E_i} est la fonction indicatrice de E_i. Alors $g+h$ est courbe si et seulement si g et h sont courbes.*

Grâce au résultat précédent, nous en déduisons plusieurs nouvelles classes de fonctions semi-courbes en forme bivariée. En effet, on peut déduire des fonctions de la classe H présentées dans le Chapitre 4 les familles suivantes :

Soit g une fonction booléenne de la classe $\mathcal{PS}_{ap}$. Soit h une des fonctions booléennes de la liste suivante ([44]) :

- $h(x,y) = \mathrm{Tr}_1^m(x^{-5}y^6)$, m impair;
- $h(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}})$, m impair:
- $h(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{-3\cdot(2^{k-1}-1)}y^{3\cdot 2^{k-1}-2})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^k-2^{2k}}y^{2^k+2^{2k}})$, $m = 4k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{2^{3k-1}-2^{2k}+2^k}y^{1-2^{3k-1}+2^{2k}-2^k})$, $m = 4k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^{2k+1}-2^{3k+1}}y^{2^{2k+1}+2^{3k+1}})$, $m = 4k+1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{2^{3k+1}-2^{2k+1}+2^k}y^{1-2^{3k+1}+2^{2k+1}-2^k})$, $m = 4k+1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{1-2^k}y^{2^k} + x^{-(2^k+1)}y^{2^k+2} + x^{-3\cdot(2^k+1)}y^{3\cdot 2^k+4})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(y(y^{2^k+1}x^{-(2^k+1)} + y^3x^{-3} + yx^{-1})^{2^{k-1}-1})$, $m = 2k-1$;
- $h(x,y) = \mathrm{Tr}_1^m(x^{\frac{5}{6}}y^{\frac{1}{6}} + x^{\frac{1}{2}}y^{\frac{1}{2}} + x^{\frac{1}{6}}y^{\frac{5}{6}})$, m impair;
- $h(x,y) = \mathrm{Tr}_1^m(x[D_{\frac{1}{5}}\left(\frac{y}{x}\right)]^6)$, m impair, où$D_{\frac{1}{5}}$ est le polynôme de Dickson d'indice $\frac{1}{5}$.

Alors la fonction $g+h$ est semi-courbe. En forme univariée, il est possible d'expliciter un peu plus ces familles de fonctions semi-courbes en donnant une expression polynomiale de certaines sous-familles. Dans ce cas, on utilise le *spread* $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ (où U est le groupe multiplicatif $\{u \in \mathbb{F}_{2^n}; u^{2^m+1} = 1\}$). En considérant ce *spread*, des fonctions dont les restrictions aux sous-espaces vectoriels $u\mathbb{F}_{2^m}$ sont linéaires sont de la forme (voir [93]) :

$$\mathrm{Tr}_1^{o((2^m-1)s+1)}\left(a_s x^{(2^m-1)s+1}\right) \text{ with } 1 \leq s \leq 2^m$$

Il est connu aussi que les fonctions dont la forme est la suivante appartiennent à la classe $\mathcal{PS}_{ap}$:

$$\sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}\left(b_r x^{(2^m-1)r}\right) \text{ where } R \subset \{1,\cdots,2^m\}.$$

En s'appuyant d'une part sur les résultats donnés par Dobbertin et al. dans [93] et d'autre part sur les résultats donnés par Charpin et Gong [54], nous avons obtenu le résultat suivant.

Corollaire 22. *Soit f une fonction booléenne dont l'expression est de la forme :*

$$f(x) = \mathrm{Tr}_1^m(a_0 x^{2^m+1}) + \sum_{i=1}^{L} \mathrm{Tr}_1^n(a_i x^{(2^m-1)s_i+1}) + \sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}(b_r x^{(2^m-1)r})$$

où L est un entier positif, $2 \le s_i \le 2^m$, $s_i \neq 2^{m-1}+1$, $1 \le r \le 2^m$, $a_0 \in \mathbb{F}_{2^m}$, $a_i \in \mathbb{F}_{2^m}$ et $b_r \in \mathbb{F}_{2^{o((2^m-1)r)}}$ (avec au moins un des coefficient $a_i \neq 0$ et un des coefficients $b_r \neq 0$). Supposons que :

1) Le nombre de racines u de $U := \{x \in \mathbb{F}_{2^n}; x^{2^m+1} = 1\}$ de l'équation $\mathrm{Tr}_m^n(cu)+\sum_{i=1}^{L} \mathrm{Tr}_m^n(a_i u^{2s_i-1})+ a_0^{\frac{1}{2}} = 0$ est égal à 0 ou 2 pour tout $c \in \mathbb{F}_{2^n}$,

2) La somme $\sum_{u\in U} \chi(\sum_{r\in R} \mathrm{Tr}_1^{o((2^m-1)r)}(b_r u^r))$ est égal à 1.
Alors, f est semi-courbe.

Par ce résultat et grâce aux résultats que nous avons obtenus sur les fonctions (hyper)-courbes, nous avons pu expliciter trente nouvelles familles infinies de fonctions semi-courbes $g_i + h_j$ ($i \in \{1,\cdots,6\}$, $j \in \{1,\cdots,5\}$) en forme univariée où g_i est une des familles ci-dessous (définies sur $\mathbb{F}_{2^n}$ et appartenant toutes à la classe $\mathcal{PS}_{ap}$) :

- $g_1(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)})$; $\gcd(r, 2^m+1) = 1$, $a \in \mathbb{F}_{2^m}^\star$ vérifiant $K_m(a) = 0$
- $g_2(x) = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$; $\gcd(r, 2^m+1) = 1$, $m > 3$ impair, $b \in \mathbb{F}_4^\star$, $a \in \mathbb{F}_{2^m}^\star$ vérifiant $K_m(a) = 4$
- $g_3(x) = \mathrm{Tr}_1^n(a\zeta^i x^{3(2^m-1)}) + \mathrm{Tr}_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m impair et $m \not\equiv 3 \pmod 6$, β est un élément primitif de $\mathbb{F}_4$, ζ est un générateur du groupe cyclique U des racines (2^m+1)-ième de l'unité, $(i,j) \in \{0,1,2\}^2$, $a \in \mathbb{F}_{2^m}^\star$ vérifiant $K_m(a) = 4$ et $\mathrm{Tr}_1^m(a^{1/3}) = 0$
- $g_4(x) = \mathrm{Tr}_1^n(a\zeta^i x^{3(2^m-1)}) + \mathrm{Tr}_1^2(\beta^j x^{\frac{2^n-1}{3}})$; m impair et $m \not\equiv 3 \pmod 6$, β est un élément primitif de $\mathbb{F}_4$, ζ est un générateur du groupe cyclique U des racines (2^m+1)-ième de l'unité, $i \in \{1,2\}$, $j \in \{0,1,2\}$, $a \in \mathbb{F}_{2^m}^\star$ vérifiant $K_m(a) + C_m(a,a) = 4$ et $\mathrm{Tr}_1^m(a^{1/3}) = 1$,
- $g_5(x) = \sum_{i=1}^{2^{m-1}-1} \mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$; $\beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$,
- $g_6(x) = \sum_{i=1}^{2^{m-2}-1} \mathrm{Tr}_1^n\left(\beta x^{i(2^m-1)}\right)$; m impair et $\beta^{(2^m-4)^{-1}} \in \{x \in \mathbb{F}_{2^m}^\star; \mathrm{Tr}_1^m(x) = 0\}$,

et h_j est une des fonctions courbes ci-dessous (dont chaque terme est une fonction monôme dont l'exposant est un exposant de Niho) :

- $h_1(x) = \mathrm{Tr}_1^m\left(a_1 x^{2^m+1}\right)$; $a_1 \in \mathbb{F}_{2^m}^\star$
- $h_2(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)3+1}\right)$;
  $a_1 \in \mathbb{F}_{2^n}^\star$, $a_2^{2^m+1} = a_1 + a_1^{2^m} = \beta^5$ avec $\beta \in \mathbb{F}_{2^n}^\star$

- $h_3(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{4}+1}\right)$;
  $a_1 \in \mathbb{F}_{2^n}^\star$ $a_2^{2^m+1} = a_1 + a_1^{2^m}$, m impair
- $h_4(x) = \mathrm{Tr}_1^n\left(a_1 x^{(2^m-1)\frac{1}{2}+1} + a_2 x^{(2^m-1)\frac{1}{6}+1}\right)$; $a_1 \in \mathbb{F}_{2^n}^\star$ $a_2^{2^m+1} = a_1 + a_1^{2^m}$, m pair
- $h_5(x) = \mathrm{Tr}_1^n\left(\alpha x^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} x^{s_i}\right)$, $r > 1$ tel que $gcd(r, m) = 1$, $\alpha \in \mathbb{F}_{2^n}$ vérifiant $\alpha + \alpha^{2^m} = 1$, $s_i = (2^m - 1)\frac{i}{2^r} \pmod{2^m + 1} + 1$, $i \in \{1, \cdots, 2^{r-1} - 1\}$

Publications

Les résultats présentés dans ce chapitre ont fait l'objet des publications suivantes :

- S. Mesnager. Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. IEEE Transactions on Information Theory-IT, Vol 57, No 11, pages 744–7458, 2011([199]).
- S. Mesnager. Semi-bent functions with multiple trace terms and hyperelliptic curves. Proceeding of International Conference on Cryptology and Information Security in Latin America (IACR), Latincrypt 2012, LNCS 7533, Springer, pages 18–36, 2012 ([200]).
- S. Mesnager et G. Cohen . On the link of some semi-bent functions with Kloosterman sums. Proceeding of International Workshop on Coding and Cryptology (IWCC 2011), LNCS 6639, pages 263–272, Springer, 2011([201]).
- C. Carlet et S. Mesnager. On Semi-bent Boolean Functions. IEEE Transactions on Information Theory-IT, Vol 58, No 5, pages 3287-3292, 2012 ([45]).

Chapitre 9

Les codes de Reed-Muller, introduits par E. Muller et L. S. Reed en 1954, sont des familles de codes les plus étudiées. A l'exception des codes de Reed-Muller d'ordre 1 ou des codes de longueurs petites, leur distance minimale, i.e. la plus petite distance entre deux mots du code, est plus petite que celle des codes BCH. L'intérêt de ces codes est qu'il existe des algorithmes efficaces de décodage associés. Ils contiennent aussi des sous-codes non-linéaires de paramètres optimaux et pour lesquels des algorithmes de décodage efficaces existent aussi. Bien qu'il ait fait l'objet de nombreux travaux, leur rayon de recouvrement est inconnu à l'exception des codes de Reed-Muller de longueur petite ou des codes de Reed-Muller d'ordre 1 de longueur 2^m avec m pair. Le rayon de recouvrement d'un code C d'un ensemble X est la valeur du plus petit rayon ρ pour lequel il est possible de recouvrir X avec des boules de Hamming de rayon ρ centrées en les mots du code. Le rayon de recouvrement représente aussi le nombre maximal d'erreurs qui peuvent être corrigées en utilisant le décodage par maximum de vraisemblance.

Il a été obtenu des bornes inférieure et supérieure pour le rayon de recouvrement des codes de Reed-Muller, mais l'écart entre ces deux bornes est très grand. Il est intéressant et important d'améliorer autant que possible ces bornes. Un ouvrage intéressant sur le rayon de recouvrement est [68] et une liste non-exhaustive de travaux sur le rayon de recouvrement est [69, 130, 131, 186, 230, 239].

Parmi les propriétés des codes de Reed-Muller, une propriété importante est que leur mots peuvent être identifiés aux supports de fonctions booléennes. Plus précisément, le code de Reed-Muller d'ordre r, noté $\mathcal{RM}(r, n)$, peut être identifié à l'ensemble des fonctions booléennes

de degré algébrique au plus r. Le rayon de recrouvrement de $\mathcal{RM}(r,n)$ coïncide alors avec la non-linéarité d'ordre r maximale. La non-linéarité d'ordre r généralise la non-linéarité standard et est définie comme la distance minimale d'une fonction booléenne à l'ensemble des fonctions booléennes de degrés algébriques au plus r. Elle quantifie la résistance d'une fonction booléenne aux attaques utilisant des approximations des fonctions booléennes par des fonctions de bas degrés [152, 234]. La nonlinéarité d'ordre r pourrait aussi donner des informations sur la résistance d'une fonction booléenne aux attaques algébriques [73, 187], comme l'a observé Carlet dans [34]. Récemment, une autre notion de rayon de recouvrement a été introduite dans le contexte des systèmes de chiffrement par flots [143, 7].

Synthèse des principaux résultats

Notre principale contribution avec C. Carlet a été d'améliorer la borne supérieure sur rayon de recouvrement du code de Reed-Muller d'ordre 2. Notre approche repose principalement sur l'introduction de sommes de caractères et sur la caractérisation des mots des codes de Reed-Muller d'ordre 2 de poids au plus deux fois et demi la distance minimale de ce code.

Théorème 23. *Pour tout entier positif $n \geq 17$, le rayon de recouvrement $\rho(2,n)$ du code de Reed-Muller $\mathcal{RM}(2,n)$ d'ordre 2 est majoré par*

$$\left\lfloor 2^{n-1} - \frac{\sqrt{15}}{2} \cdot 2^{\frac{n}{2}} \cdot \left(1 - \frac{122929}{21 \cdot 2^n} - \frac{155582504573}{4410 \cdot 2^{2n}}\right)\right\rfloor \tag{11.11}$$

Ce résultat nous a permis d'améliorer la borne sur les codes de Reed-Muller d'ordre quelconque. Jusqu'à ce résultat, la meilleure borne asymptotique connue sur le rayon de recrouvrement $\rho(r,m)$ du code de Reed-Muller d'ordre r, $r \geq 2$, était :

$$\rho(2,n) \leq 2^{n-1} - \sqrt{15}\, 2^{\frac{n}{2}-1} + O(1).$$

En utilisant l'inégalité classique

$$\rho(r,n) \leq \rho(r-1,n-1) + \rho(r,n-1),$$

nous arrivons par récurrence sur r à améliorer la borne connue et obtenons la borne supérieure asymptotique suivante :

Théorème 24. *Soit r un entier positif supérieur ou égal à 2. Le rayon de recouvrement du code de Reed-Muller d'ordre r vérifie asymptotiquement*

$$\rho(r,n) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{n/2} + O(n^{r-2}) \tag{11.12}$$

Cela faisait 15 ans qu'aucune amélioration n'avait été trouvé et, à ce jour, nos résultats n'ont pas été améliorés.

Nous terminons en expliquant schématiquement et dans les grandes lignes notre démarche pour obtenir la majoration sur le rayon de recouvrement des codes de Reed-Muller d'ordre 2. Notre idée a été de commencer par majorer le rayon de recouvrement en introduisant les sommes suivantes:

$$\mathcal{S}_k(f) = \sum_{g \in \mathcal{RM}(2,n)} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \right)^{2k}. \tag{11.13}$$

puis de montrer que

$$\forall k \geq 1, \quad \rho(2,m) \leq 2^{m-1} - \frac{1}{2} \min_{f \in \mathcal{B}_m} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}} \tag{11.14}$$

Nous avons ensuite montré, pour une fonction booléenne $f \in \mathcal{B}_m$, que

$$\begin{aligned}
&\mathcal{S}_k(f) = \#\,\mathcal{RM}(2,m)\, D_k \quad \text{if } k = 1,2,3\\
&\mathcal{S}_k(f) \#\,\mathcal{RM}(2,m) \left(D_k + N_k^{(8)} M_f^{(8)} \right) \text{if } k = 4,5\\
&\mathcal{S}_k(f) = \#\,\mathcal{RM}(2,m) \left(D_k + N_k^{(8)} M_f^{(8)} + \sum_{w=6}^{k} 2wk M_f^{(2w)} \right) \text{if } k \geq 6
\end{aligned}$$

où

- D_k est le nombre de choix possibles d'un uplet $(x_1, \cdots, x_{2k})$ $\sum_{i=1}^{2k} 1_{x_i} = 0$.
- $N_k^{(w)} = \#\mathcal{N}_g$ où $\mathrm{wt}(g) = w$ et $\mathcal{N}_g$ est le nombre de choix possibles d'un uplet $(x_1, \ldots, x_{2k})$ d'éléments de $\mathbb{F}_2^m$ tels que $\sum_{i=1}^{2k} 1_{x_i} = g$.
- $M_f^{(w)}$ est une somme de caractère sur les mots de $\mathcal{RM}(2,m)^{\perp}$, c'est-à-dire le code de Reed-Muller $\mathcal{RM}(m-3,m)$, de poids de Hamming w.

Pour calculer les valeurs des nombres D_k et $N_k^{(w)}$, nous introduisons des séries génératrices et montrons que ($[z^{2k}]A(z)$ désigne le coefficient de $\frac{z^{2k}}{2k!}$ dans le développement de Taylor de A en $z = 0$) :

$$\begin{aligned}
D_k &= [z^{2k}] \cosh^{2^n}(z)\\
N_k^{(2w)} &= [z^{2k}] \tanh^{2w} \cosh^{2^n}(z)
\end{aligned}$$

Maintenant, on voit qu'obtenir une borne supérieure sur $\rho(2,m)$ revient à trouver une borne inférieure sur $min_{f \in \mathcal{B}_m} \sqrt{\frac{\mathcal{S}_{k+1}(f)}{\mathcal{S}_k(f)}}$. Pour cela, nous utilisons les caractérisations connues dans la littérature des mots du code $\mathcal{RM}(m-3,m)$.

Publications

Les premiers résultats furent annoncés à la conférence ISIT. Les résultats présentés dans ce chapitre ont été publiés à IEEE-IT:

- C. Carlet et S. Mesnager. "Improving the upper bounds on the covering radii of binary Reed-Muller codes". IEEE Transactions on Information Theory, vol. 53, no. 1, pages, 162–173, 2007([43]).