Vectorial Boolean Functions for Cryptography

Claude Carlet*

This chapter is dedicated to the memory of Hans Dobbertin.

*LAGA, University of Paris 8, France; e-mail: claude.carlet@univ-paris8.fr.

Contents

1 Introduction

This chapter deals with multi-output Boolean functions viewed from a cryptographic viewpoint, that is, functions from the vectorspace $\mathbb{F}_2^n$, of all binary vectors of length n, to the vectorspace $\mathbb{F}_2^m$, for some positive integers n and m, where $\mathbb{F}_2$ is the finite field with two elements[1]. Obviously, these functions include the (single-output) Boolean functions which correspond to the case $m = 1$. The present chapter follows the chapter "Boolean Functions for Cryptography and Error Correcting Codes" (dedicated to Boolean functions), to which we refer for all the definitions and properties which will be needed in the present chapter. As in this previous chapter, additions of bits performed in characteristic 0 (that is, in $\mathbb{Z}$, *i.e.* not modulo 2) will be denoted by $+$, and additions modulo 2 (in $\mathbb{F}_2$) will be denoted by $\oplus$. The multiple sums will be denoted by $\sum_i$ when they are calculated in characteristic 0 and by $\bigoplus_i$ when they are calculated modulo 2. These two different notations are necessary because some representations of (vectorial) Boolean functions live in characteristic 2 and some representations of the same functions live in characteristic 0. However, the additions of elements of the finite field $\mathbb{F}_{2^n}$ will be denoted by $+$, as it is usual in mathematics, despite the fact they are performed in characteristic 2. 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 $n > 1$.

Let n and m be two positive integers. The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called *(n, m)-functions*. Such function F being given, the Boolean functions $f_1, \ldots, f_m$ defined, at every $x \in \mathbb{F}_2^n$, by $F(x) = (f_1(x), \ldots, f_m(x))$, are called the *coordinate functions* of F. When the numbers m and n are not specified, (n, m)-functions are called *multi-output Boolean functions*, *vectorial Boolean functions* or *S-boxes*[2] (this last term is the most often used in cryptography, but is dedicated to the vectorial functions whose role is to provide confusion into the system; see the subsection on the cryptographic criteria for Boolean functions in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" for the meaning of this term).

S-boxes are parts of iterative *block ciphers* and they play a central role in their robustness. Iterative block ciphers are the iterations of a transformation depending on a key over each block of plaintext. The iterations are called rounds and the key used in an iteration is called a round key. The round keys are computed from the secret key (called the master key) by a

[1] Denoted by $\mathcal{B}$ in some chapters of the present collection.

[2] "S" for "Substitution".

key scheduling algorithm. The rounds consist of vectorial Boolean functions combined in different ways involving the round key. Figures displaying the location of the S-boxes in the two main block ciphers, DES and AES, can be found in the chapter "Boolean Functions for Cryptography and Error Correcting Codes".

The main attacks on block ciphers, which will result in design criteria, are the following.

The *differential attack*, introduced by Biham and Shamir [11], assumes the existence of ordered pairs (α, β) of binary strings of the same length as the blocks (which are binary strings too), such that, a block m of plaintext being randomly chosen and c and c' being the cipher texts related to m and $m+\alpha$, the bitwise difference $c+c'$ (recall that we use $+$ to denote the bitwise addition/difference in $\mathbb{F}_2^n$) has a larger probability to be equal to β than if c and c' were binary strings randomly chosen; such an ordered pair (α, β) is called a differential; the larger the probability of the differential, the more efficient is the attack. The related criterion on an (n, m)-function F used as an S-box in the round functions of the cipher is that the output to its derivatives $D_a(x) = F(x) + F(x+a)$; $x, a \in \mathbb{F}_2^n$, must be as uniformly distributed as possible (except for the case $a = 0$, obviously). There are several ways to mount the differential cryptanalysis. The most common (and most efficient) one is to use differentials for the *reduced cipher*, that is, the input to the last round (*i*.e. the cipher obtained from the original one by removing its last round); this allows, *see figure 1 below*, to distinguish, in a *last round attack*, the reduced cipher from a random permutation; the existence of such *distinguisher* allows recovering the key used in the last round (either by an exhaustive search, which is efficient if this key is shorter than the master key, or by using specificities of the cipher allowing replacing the exhaustive search by, for instance, solving algebraic equations).

The *linear attack*, introduced by Matsui [131] is based on an idea from [153]. Its most common version is also an attack on the reduced cipher. It uses as distinguishers triples (α, β, γ) of binary strings such that, a block m of plaintext and a key k being randomly chosen, the bit $\alpha \cdot m \oplus \beta \cdot c \oplus \gamma \cdot k$, where "$\cdot$" denotes the usual inner product, has a probability different from $1/2$ of being null. The more distant from $1/2$ the probability is, the more efficient is the attack. The related criterion on the S-boxes used in the round functions of the cipher deals with the so-called *component functions*, which are the linear combinations, with non all-zero coefficients, of the coordinate functions of the S-box (their set is the vector space spanned by the coordinate functions, deprived of the null function if the coordinate functions are $\mathbb{F}_2$-linearly independent). The nonlinearities (see definition in the chapter

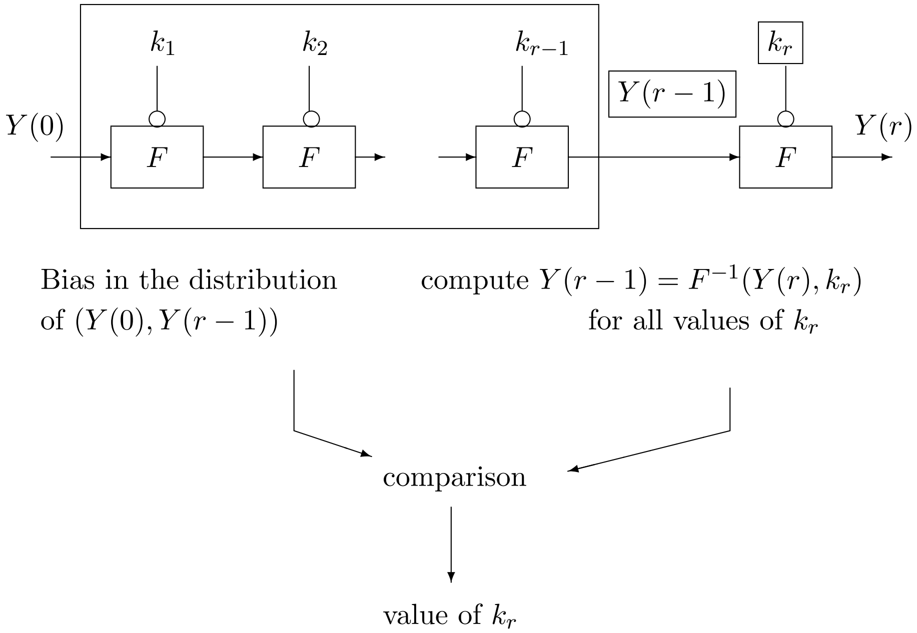
k_1
k_2
k_{r-1}
k_r
$Y(r-1)$
$Y(0)$
F
F
F
F
$Y(r)$
Bias in the distribution of $(Y(0), Y(r-1))$
compute $Y(r-1) = F^{-1}(Y(r), k_r)$ for all values of k_r
comparison
value of k_r

Figure 1: Last round attacks

"Boolean Functions for Cryptography and Error Correcting Codes" or see below) of all these component functions must be as high as possible. The design of the AES has been partly founded on the studies (by K. Nyberg and others) on the notions of nonlinearity (for the resistance to linear attacks) and differential uniformity (for the resistance to differential attacks). This has allowed the AES to use S-boxes working on bytes (it would not have been possible to find a good 8-bit-to-8-bit S-box by a computer search as this had been done for the 6-bit-to-4-bit S-boxes of the DES).
The *higher order differential attack* [124, 118] exploits the fact that the algebraic degree of the S-box F is low, or more generally that there exists a low dimensional vector subspace V of $\mathbb{F}_2^n$ such that the function $D_V F(x) = \sum_{v \in V} F(x+v)$ is constant. A probabilistic version of this attack [109] allows the derivative not to be constant and the S-box must then have high "higher order nonlinearity" (see Subsection 3.2 on this notion).

The *interpolation attack* [110] is efficient when the degree of the univariate polynomial representation of the S-box over $\mathbb{F}_{2^n}$ – see the next section – is low or when the distance of the S-box to the set of low univariate degree functions is small.
Algebraic attacks also exist on block ciphers (see *e.g.* [73]), exploiting the existence of multivariate equations involving the input to the S-box and its output (an example of such equation is $x^2y = x$ in the case of the AES), but their efficiency has to be more precisely studied: the number of variables in the resulting system of equations, which equals the global number of data bits and of key bits in all rounds of the cipher, is much larger than for stream ciphers and the resulting systems of equations are not as overdefined as for stream ciphers. However, the AES allowing bilinear relations between the input and the output bits to the S-boxes[3], this may represent a thread.
The *Slide attack* [12], when it can be mounted, has a complexity independent of the number of rounds in the block cipher, contrary to the attacks previously described. It analyzes the weaknesses of the key schedule (the most common case of weakness being when round keys repeat in a cyclic way) to break the cipher. The slide attack is efficient when the cipher can be decomposed into multiple rounds of an identical F function vulnerable to a known-plaintext attack.

In the *pseudo-random generators* of *stream ciphers*, (n, m)-functions can be used to combine the outputs to n linear feedback shift registers (LFSR), or to filter the content of a single one, generating then m bits at each clock cycle instead of only one, which increases the speed of the cipher (but risks decreasing its robustness). The attacks, described in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", are obviously also efficient on these kinds of ciphers. They are in fact often more efficient (see Subsection 3.3).

2 Generalities on vectorial Boolean functions

2.1 The Walsh transform

We shall call *Walsh transform* of an (n, m)-function F the function which maps any ordered pair $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ to the value at u of the Walsh transform of the component[4] function $v \cdot F$, that is, $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$.

[3] It is possible to avoid such relations when the number of input/output bits is 8, if non-power S-boxes are used (but this may have a cost in terms of speed).

[4] Properly speaking, we can use the term of component function only for $v \neq 0$; so we make an abuse, here.

If we denote by G_F the graph $\{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^m / \, y=F(x)\}$ of F, and by 1_{G_F} its indicator (taking value 1 on G_F and 0 outside), then we have $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}=\widehat{1_{G_F}}(u,v)$, where $\widehat{1_{G_F}}$ is the Fourier transform of the Boolean function 1_{G_F} (see the definition of the Fourier transform in the previous chapter). This observation gives more insight on what is the Walsh transform and it gives moreover a convenient notation for denoting it.

Observation *The Walsh transform of any vectorial function is the Fourier transform of the indicator of its graph.*

There is a simple way of expressing the value of the Walsh transform of the composition of two vectorial functions by means of those of the functions:

Proposition 1 *If we write the values of the function $\widehat{1_{G_F}}$ in a $2^m\times 2^n$ matrix (in which the term located at the row indexed by $v\in\mathbb{F}_2^m$ and at the column indexed by $u\in\mathbb{F}_2^n$ equals $\widehat{1_{G_F}}(u,v)$), then, the matrix corresponding to the composition $F\circ H$ of F, where H is an (r,n)-function, equals the product (in the same order) of the matrices associated to F and H, divided by 2^n.*

Proof. For every $w\in\mathbb{F}_2^r$ and every $v\in\mathbb{F}_2^m$, we have

$$\begin{aligned}\sum_{u\in\mathbb{F}_2^n}\widehat{1_{G_F}}(u,v)\widehat{1_{G_H}}(w,u) &= \sum_{u\in\mathbb{F}_2^n;x\in\mathbb{F}_2^r;y\in\mathbb{F}_2^n}(-1)^{v\cdot F(y)\oplus u\cdot y\oplus u\cdot H(x)\oplus w\cdot x}\\ &= 2^n\sum_{x\in\mathbb{F}_2^r;y\in\mathbb{F}_2^n\,/\,y=H(x)}(-1)^{v\cdot F(y)\oplus w\cdot x}\\ &= 2^n\widehat{1_{G_{F\circ H}}}(w,v),\end{aligned}$$

since $\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot y\oplus u\cdot H(x)}$ equals 2^n if $y=H(x)$, and is null otherwise. □

Remark. Because of Proposition 1, it could seem more convenient to exchange the positions of u and v in $\widehat{1_{G_F}}(u,v)$, in order to have the row index first. However, it seems to us more natural to respect the order (input,output).

We shall call *Walsh spectrum* of F the multi-set of all the values of the Walsh transform of F, *i.e.* $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ where $u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^{m*}$ (where $\mathbb{F}_2^{m*}=\mathbb{F}_2^m\setminus\{0\}$). We shall call *extended Walsh spectrum* of F the multi-set of their absolute values, and *Walsh support* of F the set of those (u,v) such that $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\neq 0$.

Remark. We have

$$\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}=\sum_{b\in\mathbb{F}_2^m}\widehat{\varphi_b}(u)(-1)^{v\cdot b} \qquad (1)$$

where $\widehat{\varphi_b}$ is the discrete Fourier transform of the indicator function φ_b of the pre-image $F^{-1}(b)=\{x\in\mathbb{F}_2^n/\, F(x)=b\}$, defined by $\varphi_b(x)=1$ if $F(x)=b$ and $\varphi_b(x)=0$ otherwise.

2.2 The different ways of representing vectorial functions

2.2.1 The Algebraic Normal Form

The notion of *algebraic normal form* of Boolean functions can easily be extended to (n,m)-functions. Since each coordinate function of such a function F is uniquely represented as a polynomial on n variables, with coefficients in $\mathbb{F}_2$ and in which every variable appears in each monomial with degree 0 or 1, the function F itself is uniquely represented as a polynomial of the same form with coefficients in $\mathbb{F}_2^m$, or more precisely as an element of $\mathbb{F}_2^m[x_1,\cdots,x_n]/(x_1^2\oplus x,\cdots,x_n^2\oplus x)$:

$$F(x)=\sum_{I\in\mathcal{P}(N)}a_I\left(\prod_{i\in I}x_i\right)=\sum_{I\in\mathcal{P}(N)}a_I\,x^I, \qquad (2)$$

where $\mathcal{P}(N)$ denotes the power set of $N=\{1,\ldots,n\}$, and a_I belongs to $\mathbb{F}_2^m$ (according to our convention on the notation for additions, we used $\sum$ to denote the sum in $\mathbb{F}_2^m$, but recall that, coordinate by coordinate, this sum is a $\bigoplus$). This polynomial is called again the algebraic normal form (ANF) of F. Keeping the i-th coordinate of each coefficient in this expression gives back the ANF of the i-th coordinate function of F. Moreover, according to the relations recalled in the chapter “Boolean Functions for Cryptography and Error Correcting Codes”, a_I equals $\sum_{x\in\mathbb{F}_2^n/\,supp(x)\subseteq I}F(x)$ (this sum being calculated in $\mathbb{F}_2^n$) and conversely, we have $F(x)=\sum_{I\subseteq supp(x)}a_I$.
The *algebraic degree* of the function is by definition the global degree of its ANF: $d^\circ F=\max\{|I|/\,a_I\neq(0,\ldots,0);I\in\mathcal{P}(N)\}$. It therefore equals the maximal algebraic degree of the coordinate functions of F. It also equals the maximal algebraic degree of the component functions of F. It is a right and left *affine invariant* (that is, its value does not change when we compose F, on the right or on the left, by an affine automorphism). Another notion of degree is also relevant to cryptography (and is also affine invariant): the

minimum algebraic degree of all the component functions[5] of F, often called the *minimum degree*.

2.2.2 The representation as a univariate polynomial over $\mathbb{F}_{2^n}$

A second representation of (n,m)-functions exists when $m=n$: we endow $\mathbb{F}_2^n$ with the structure of the field $\mathbb{F}_{2^n}$, as explained in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" (see "The trace representation", in Subsection 2.1); any (n,n)-function F then admits a unique *univariate polynomial representation* over $\mathbb{F}_{2^n}$, of degree at most 2^n-1:

$$F(x)=\sum_{j=0}^{2^n-1}\delta_j x^j\ ,\quad \delta_j\in\mathbb{F}_{2^n}\ . \tag{3}$$

Indeed, the mapping which maps any such polynomial to the corresponding (n,n)-function is $\mathbb{F}_{2^n}$-linear and has kernel $\{0\}$, since a nonzero univariate equation of degree at most 2^n-1 over a field can not have more than 2^n-1 solutions. The dimensions of the vectorspaces over $\mathbb{F}_{2^n}$ of, respectively, all such polynomials, and all (n,n)-functions, being both equal to 2^n, this mapping is bijective. Note that the univariate representation (3) of F can be obtained by expanding and simplifying the expression:

$$\sum_{a\in\mathbb{F}_{2^n}}F(a)(1+(x+a)^{2^n-1}).$$

The way to obtain the ANF from this univariate polynomial is similar to the case of Boolean functions seen in the previous chapter; we recall it for self-completeness: for every binary vector $x\in\mathbb{F}_2^n$, we can also denote by x the element $\sum_{i=1}^n x_i\alpha_i$ of $\mathbb{F}_{2^n}$, where $(\alpha_1,\ldots,\alpha_n)$ is a basis of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_{2^n}$. Let us write the *binary expansion* of every integer $j\in[0;2^n-1]$: $\sum_{s=0}^{n-1}j_s2^s$, $j_s\in\{0,1\}$. We have:

$$\begin{aligned}F(x)&=\sum_{j=0}^{2^n-1}\delta_j\left(\sum_{i=1}^n x_i\alpha_i\right)^j\\&=\sum_{j=0}^{2^n-1}\delta_j\left(\sum_{i=1}^n x_i\alpha_i\right)^{\sum_{s=0}^{n-1}j_s2^s}\\&=\sum_{j=0}^{2^n-1}\delta_j\prod_{s=0}^{n-1}\left(\sum_{i=1}^n x_i\alpha_i^{2^s}\right)^{j_s}\end{aligned}$$

[5] Not just the coordinate functions; the notion would then not be affine invariant.

since the mapping $x \to x^2$ is $\mathbb{F}_2$-linear over $\mathbb{F}_{2^n}$ and $x_i \in \mathbb{F}_2$. Expanding these last products, simplifying and decomposing again over the basis $(\alpha_1, \dots, \alpha_n)$ gives the ANF of F.
Another method is the Lagrange interpolation theorem.
It is then possible to read the algebraic degree of F directly on the univariate polynomial representation: let us denote by $w_2(j)$ the number of nonzero coefficients j_s in the binary expansion $\sum_{s=o}^{n-1} j_s 2^s$ of j, *i*.e. $w_2(j) = \sum_{s=0}^{n-1} j_s$. The number $w_2(j)$ is called the *2-weight* of j. Then, the function F has algebraic degree $\max_{j=0,\dots,2^n-1/\,\delta_j \neq 0} w_2(j)$. Indeed, according to the above equalities, the algebraic degree of F is clearly bounded above by this number, and it can not be strictly smaller, because the number $2^{n\sum_{i=0}^{d}\binom{n}{i}}$ of those (n, n)-functions of algebraic degrees at most d equals the number of those univariate polynomials $\sum_{j=0}^{2^n-1} \delta_j x^j$, $\delta_j \in \mathbb{F}_{2^n}$, such that $\max_{j=0,\dots,2^n-1/\,\delta_j \neq 0} w_2(j) \leq d$.
In particular, F is $\mathbb{F}_2$-linear (resp. affine) if and only if $F(x)$ is a *linearized polynomial* over $\mathbb{F}_{2^n}$: $\sum_{j=0}^{n-1} \delta_j x^{2^j}$, $\delta_j \in \mathbb{F}_{2^n}$ (resp. a linearized polynomial plus a constant).
- If m is a divisor of n, then any (n, m)-function F can be viewed as a function from $\mathbb{F}_{2^n}$ to itself, since $\mathbb{F}_{2^m}$ is a sub-field of $\mathbb{F}_{2^n}$. Hence, the function admits a univariate polynomial representation. Note that this unique polynomial can be represented in the form $tr_{n/m}(\sum_{j=0}^{2^n-1} \delta_j x^j)$, where $tr_{n/m}(x) = x + x^{2^m} + x^{2^{2m}} + x^{2^{3m}} + \cdots + x^{2^{n-m}}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. Indeed, there exists a function G from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ such that F equals $tr_{n/m} \circ G$ (for instance, $G(x) = \lambda F(x)$, where $tr_{n/m}(\lambda) = 1$). But there is no uniqueness of G in this representation.

2.2.3 The multidimensional Walsh transform

K. Nyberg defines in [141] a polynomial representation, called the *multidimensional Walsh transform*; let us define:

$$\mathcal{W}(F)(z_1, \cdots, z_m) = \sum_{x \in \mathbb{F}_2^n} \prod_{j=1}^{m} z_j^{f_j(x)} \in \mathbb{Z}[z_1, \cdots, z_m]/(z_1^2 - 1, \cdots, z_m^2 - 1),$$

where $f_1, \cdots, f_m$ are the coordinate functions of F. The multidimensional Walsh transform maps every linear (n, m)-function L to the polynomial $\mathcal{W}(F + L)(z_1, \cdots, z_m)$. This is a representation with uniqueness of F, since, for every L, the knowledge of $\mathcal{W}(F + L)$ is equivalent to that of the evaluation of $\mathcal{W}(F + L)$ at $(\chi_1, \cdots, \chi_m)$ for every choice of χ_j, $j = 1, \cdots, m$, in the set $\{-1, 1\}$ of roots of the polynomial $z_j^2 - 1$. For such a choice, let us define the vector $v \in \mathbb{F}_2^m$ by $v_j = 1$ if $\chi_j = -1$ and $v_j = 0$ otherwise. For every $j = 1, \cdots, m$, let us denote by a_j the vector of $\mathbb{F}_2^n$ such that the j-th coordinate of $L(x)$ equals $a_j \cdot x$. We denote then by u the vector $\sum_{j=1}^m v_j a_j \in \mathbb{F}_2^n$. Then this evaluation equals $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$. We see that the correspondence between the multidimensional Walsh transform and the Walsh transform is the correspondence between a multi-variate polynomial of $\mathbb{Z}[z_1, \cdots, z_m]/(z_1^2 - 1, \cdots, z_m^2 - 1)$ and its evaluation over $\{(z_1, \cdots, z_m) \in \mathbb{Z}^m \,/\, z_1^2 - 1 = \cdots = z_m^2 - 1 = 0\} = \{-1, 1\}^m$. Consequently, the multidimensional Walsh transform satisfies a relation equivalent to the Parseval's relation (see [141]).

2.3 Balanced functions

As for Boolean functions, balancedness plays an important role for vectorial Boolean functions in cryptography. An (n, m)-function F is called *balanced* if it takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times. By definition, F is balanced if every function φ_b has Hamming weight 2^{n-m}.
Obviously, the balanced (n, n)-functions are the permutations on $\mathbb{F}_2^n$.

2.3.1 Characterization through the component functions

The balanced S-boxes (and among them, the permutations) can be nicely characterized by the balancedness of their component functions:

Proposition 2 *[129] An (n, m)-function is balanced if and only if its component functions are balanced, that is, if and only if, for every nonzero $v \in \mathbb{F}_2^m$, the Boolean function $v \cdot F$ is balanced.*

Proof. The relation:

$$\sum_{v\in\mathbb{F}_2^m}(-1)^{v\cdot(F(x)+b)} = \left\{\begin{array}{l} 2^m \text{ if } F(x) = b \\ 0 \text{ otherwise} \end{array}\right. = 2^m\,\varphi_b(x), \tag{4}$$

is valid for every (n, m)-function F, every $x \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, since the function $v \mapsto v \cdot (F(x) + b)$ being linear, it is either balanced or null. Thus:

$$\sum_{x\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m}(-1)^{v\cdot(F(x)+b)} = 2^m\,|F^{-1}(b)| = 2^m\; w_H(\varphi_b), \tag{5}$$

where w_H denotes the Hamming weight as in the previous chapter. Hence, the discrete Fourier transform of the function $v \mapsto \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)}$ equals the function $b \mapsto 2^m\; |F^{-1}(b)|$. We know (see the previous chapter) that a pseudo-Boolean function has constant Fourier transform if and only if it is null at every nonzero vector. We deduce that F is balanced if and only if the function $v \mapsto \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)}$ is null on ${\mathbb{F}_2^m}^*$. $\square$

2.4 Generalizations to vectorial functions of notions on Boolean functions

The most important notion on Boolean functions is the nonlinearity. We devote the whole Section 3 to its generalization to S-boxes. We also devote a section (Section 4) to the notion of resiliency of vectorial functions.

2.4.1 Covering sequences

The notion of covering sequence of a balanced Boolean function has been generalized to vectorial functions and the properties of this generalization have been studied in [63].

2.4.2 Algebraic immunity

The notion of *algebraic immunity* of S-boxes has been studied in [1, 2]. As recalled in the introduction, the existence of multivariate relations of low degrees between the input bits and the output bits may be exploited in algebraic attacks [73] (but contrary to the case of stream ciphers, the system of equations is generally not overdefined). Several notions of algebraic immunity of an S-box F have been related to these attacks. We first recall the definition of annihilator and we give the definition of the algebraic immunity of a set:

Definition 1 *We call* annihilator *of a subset E of $\mathbb{F}_2^n$ any n-variable Boolean function vanishing on E. We call algebraic immunity of E, and we denote by $AI(E)$, the minimum algebraic degree of all the non-zero annihilators of E.*

The algebraic immunity of a Boolean function f (see the previous chapter) equals by definition $\min(AI(f^{-1}(0)), AI(f^{-1}(1)))$.
The first generalization of algebraic immunity to S-boxes is its direct extension:

Definition 2 *The* basic algebraic immunity $AI(F)$ *of any (n, m)-function F is the minimum algebraic immunity of all the pre-images $F^{-1}(z)$ of elements z of $\mathbb{F}_2^m$ by F.*

Note that $AI(F)$ also equals the minimum algebraic immunity of all the indicators φ_z of the pre-images $F^{-1}(z)$ since, the algebraic immunity being a non-decreasing function over sets, we have for every $z \in \mathbb{F}_2^m$:

$$AI(\mathbb{F}_2^n \setminus F^{-1}(z)) \geq AI(F^{-1}(z')), \forall z \neq z'.$$

This notion has an interest only for sufficiently small values of m (for instance, for S-boxes used in stream ciphers), see below. A second notion of algebraic immunity of S-boxes, more relevant when m is comparable to n (which is the case of S-boxes used in block ciphers) has been called the *graph algebraic immunity* and is defined as follows:

Definition 3 *The graph algebraic immunity of any (n, m)-function F is the algebraic immunity of the graph $\{(x, F(x));\ x \in \mathbb{F}_2^n\}$ of the S-box.*

This second notion will be denoted by $AI_{gr}(F)$.
Two other notions have been studied in [2] but it is proved in [128] that they are in fact different expressions for the same $AI(F)$ and $AI_{gr}(F)$.
A third notion, that we shall call the *component algebraic immunity*, seems also natural:

Definition 4 *The component algebraic immunity of any (n, m)-function F is the minimal algebraic immunity of the component functions $v \cdot F$ ($v \neq 0$ in $\mathbb{F}_2^m$) of the S-box.*

We shall denote it by $AI_{comp}(F)$.

Properties It has been observed in [1] that, for any (n, m)-function F, we have $AI(F) \leq AI_{gr}(F) \leq AI(F) + m$. The left-hand side inequality is straightforward (by restricting an annihilator of the graph to a value of y such that the annihilator does not vanish for every x) and the right-hand side inequality comes from the fact that, since there exists z and a non-zero annihilator $g(x)$ of $F^{-1}(z)$ of algebraic degree $AI(F)$, the function $g(x) \prod_{i=1}^{m} (y_j \oplus z_j \oplus 1)$ is an annihilator of algebraic degree $AI(F) + m$ of the graph of F.
It has been also observed in [1] that, denoting by d the smallest integer such that $\sum_{i=0}^{d} \binom{n}{i} > 2^{n-m}$, we have $AI(F) \leq d$ (indeed, there is at least one z such that $|F^{-1}(z)| \leq 2^{n-m}$, the annihilators of $F^{-1}(z)$ are the solutions of $|F^{-1}(z)|$ linear equations in $\sum_{i=0}^{d} \binom{n}{i}$ unknowns - which are the coefficients of the ANF of an unknown annihilator of degree at most d - and the number of equations being strictly smaller than the number of unknowns, the system must have non-trivial solutions). It has been

proved in [95] (among other results) that this bound is tight. Note that it shows that the basic algebraic immunity has no relevance when m is not small enough: we need $m \leq n - \log_2(n+1)$ for $AI(F)$ being possibly greater than 1; more generally, we know (see [130], page 310) that $\sum_{i=0}^{d} \binom{n}{i} \geq \frac{2^{nH_2(d/n)}}{\sqrt{8d(1-d/n)}}$, where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$; hence, for $AI(F)$ being possibly greater than a number k, we must have $m \leq n\,(1 - H_2(k/n)) + \frac{1}{2}\,(3 + \log_2(k(1-k/n)))$.
Finally, it has also been proved in [1] that, denoting by D the smallest integer such that $\sum_{i=0}^{D} \binom{n+m}{i} > 2^n$, we have $AI_{gr}(F) \leq D$ (the proof is similar, considering annihilators in $n+m$ variables - the input coordinates and the output coordinates - of the graph) but it is not known whether this bound is tight (it is shown in [1] that it is tight for $n \leq 14$ and partially for $n = 15$).

Since the algebraic immunity of any Boolean function is bounded above by its algebraic degree, the component algebraic immunity of any vectorial function is bounded above by its minimum degree and therefore by its algebraic degree:

$$AI_{comp}(F) \leq d^\circ F.$$

We have also:

$$AI_{comp}(F) \geq AI(F),$$

since $AI_{comp}(F)$ equaling the algebraic immunity of the Boolean function $v \cdot F$ for some $v \neq 0$, it equals $AI(F^{-1}(H))$ for some affine hyperplane H of $\mathbb{F}_2^m$, and AI is a non-decreasing function over sets. We have:

$$AI_{comp}(F) \geq AI_{gr}(F) - 1$$

since:
- if g is a nonzero annihilator of $v \cdot F$, $v \neq 0$, then the product $h(x,y) = g(x)\,(v \cdot y)$ is a nonzero annihilator of the graph of F;
- if g is a nonzero annihilator of $v \cdot F \oplus 1$ then $h(x,y) = g(x)\,(v \cdot y) \oplus g(x)$ is a nonzero annihilator of the graph of F.

3 Highly nonlinear vectorial Boolean functions

3.1 Nonlinearity of S-boxes in block ciphers

A generalization to (n,m)-functions of the notion of nonlinearity of Boolean functions has been introduced and studied by Nyberg [136] and further studied by Chabaud and Vaudenay [65]:

Definition 5 *The* nonlinearity $nl(F)$ *of an* (n,m)*-function* F *is the minimum nonlinearity of all the component functions* $x \in \mathbb{F}_2^n \mapsto v\cdot F(x)$, $v \in \mathbb{F}_2^m$, $v \neq 0$.

In other words, $nl(F)$ equals the minimum Hamming distance between all the component functions of F and all affine functions on n variables. As we saw in the introduction, this generalization quantifies the level of resistance of the S-box to the linear attack.

The nonlinearity of S-boxes is clearly a right and left affine invariant (that is, it does not change when we compose F by affine automorphisms) and the nonlinearity of an S-box F does not change if we add to F an affine function. Moreover, if A is a surjective linear (or affine) function from $\mathbb{F}_2^p$ (where p is some positive integer) into $\mathbb{F}_2^n$, then it is easily shown that $nl(F \circ A) = 2^{p-n} nl(F)$, since by affine invariance, we can assume without loss of generality that A is a projection.

According to the equality relating the nonlinearity of a Boolean function to the maximal magnitude of its Walsh transform, we have:

$$\begin{aligned} nl(F) &= 2^{n-1} - \frac{1}{2} \max_{v\in\mathbb{F}_2^{m*};\ u\in\mathbb{F}_2^n} \left| \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot F(x)\oplus u\cdot x} \right| \qquad (6) \\ &= 2^{n-1} - \frac{1}{2} \max_{v\in\mathbb{F}_2^{m*};\ u\in\mathbb{F}_2^n} \left| \widehat{1_{G_F}}(u,v) \right|. \end{aligned}$$

Note that "$\max\limits_{v\in\mathbb{F}_2^{m*};\ u\in\mathbb{F}_2^n}$" can be replaced by "$\max\limits_{(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^m;(u,v)\neq(0,0)}$", since we have $\sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot x} = 0$ for every nonzero u. Hence, if $n=m$ and if F is a permutation, then F and its inverse F^{-1} have the same nonlinearity (change the variable x into $F^{-1}(x)$.

Relation with linear codes As observed in [56, 156], there is a relationship between the maximal possible nonlinearity of (n,m)-functions and the possible parameters of the linear supercodes of the Reed-Muller code of order 1. Let C be a linear $[2^n, K, D]$ binary code including the Reed-Muller code $RM(1,n)$ as a subcode. Let $(b_1,\dots,b_K)$ be a basis of C completing a basis $(b_1,\dots,b_{n+1})$ of $RM(1,n)$. The n-variable Boolean functions corresponding to the vectors $b_{n+2},\dots,b_K$ are the coordinate functions of an $(n, K-n-1)$-function whose nonlinearity is D. Conversely, if $D > 0$ is the nonlinearity of some (n,m)-function, then the linear code equal to the union of the cosets $v\cdot F + RM(1,n)$, where v ranges over $\mathbb{F}_2^m$, has parameters $[2^n, n+m+1, D]$. Existence and non-existence results[6] on highly nonlinear vectorial functions are deduced in [156] and upper bounds on the nonlinearity of (n,m)-functions are derived in [58].

3.1.1 The covering radius bound; bent/perfect nonlinear functions

The covering radius bound being valid for every n-variable Boolean function (see the previous chapter), it is *a fortiori* valid for every (n,m)-function:

$$nl(F) \leq 2^{n-1} - 2^{n/2-1}. \tag{7}$$

Definition 6 *An (n,m) function is called* bent *if it achieves the covering radius bound* (7) *with equality.*

The notion of bent vectorial function is invariant under composition on the left and on the right by affine automorphisms and by addition of affine functions. Clearly, an (n,m)-function is bent if and only if all of the component functions $v \cdot F$, $v \neq 0$ of F are bent (*i.e.* achieve the same bound[7]). Hence, the algebraic degree of any bent (n,m)-function is at most $n/2$. Note also that, since any n-variable Boolean function f is bent if and only if all of its derivatives $D_af(x) = f(x) \oplus f(x+a)$, $a \neq 0$, are balanced, an (n,m)-function F is bent if and only if, for every $v \in \mathbb{F}_2^m$, $v \neq 0$, and every $a \in \mathbb{F}_2^n$, $a \neq 0$, the function $v \cdot (F(x) + F(x+a))$ is balanced. According to Proposition 2, this implies:

Proposition 3 *An (n,m)-function is bent if and only if all of its* derivatives *$D_aF(x) = F(x) + F(x+a)$, $a \in \mathbb{F}_2^{n*}$, are balanced.*

For this reason, bent functions are also called *perfect nonlinear*[8]; they contribute then also to an optimum resistance to the differential attack (see introduction) of those cryptosystems in which they are involved (but they are not balanced). They can be used to design *authentication schemes* (or codes); see [66].

Thanks to the observations made in Subsection 2.2 (where we saw that the evaluation of the multidimensional Walsh transform corresponds in fact to

[6] Using the linear programming bound due to Delsarte.

[7] In other words, the existence of a bent (n,m)-function is equivalent to the existence of an m-dimensional vector space of n-variable Boolean bent functions.

[8] We shall see that perfect nonlinear (n,n)-functions do not exist; but they do exist in other characteristics than 2 (see *e.g.* [57]); they are then often called *planar*.

the evaluation of the Walsh transform), it is a simple matter to characterize the bent functions as those functions whose squared expression of the multidimensional Walsh transform at L is the same for every L.

Note that, according to the results recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", if a bent (n, m)-function F is normal in the sense that it is null on (say) an $n/2$-dimensional vector space E, then F is balanced on any translate of E. Indeed, for every $v \neq 0$ in $\mathbb{F}_2^m$ and every $u \in \mathbb{F}_2^n \setminus E$, the function $v \cdot F$ is balanced on $u + E$.

Existence of bent (n, m)-functions: since bent n-variable Boolean functions exist only if n is even, bent (n, m)-functions exist only under this same hypothesis. But, as shown by Nyberg in [135], this condition is not sufficient for the existence of bent (n, m)-functions. Indeed, we have seen in Relation (5) that, for every (n, m)-function F and any element $b \in \mathbb{F}_2^m$, the size of $F^{-1}(b)$ is equal to $2^{-m} \sum_{x\in\mathbb{F}_2^n; v\in\mathbb{F}_2^m} (-1)^{v\cdot(F(x)+b)}$. Assuming that F is bent and denoting, for every $v \in \mathbb{F}_2^{n*}$, by $\widetilde{v \cdot F}$ the dual of the bent Boolean function $x \mapsto v \cdot F(x)$, we have, by definition: $\sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot F(x)} = 2^{n/2} (-1)^{\widetilde{v\cdot F}(0)}$. The size of $F^{-1}(b)$ equals then $2^{n-m} + 2^{n/2-m} \sum_{v\in\mathbb{F}_2^{n*}} (-1)^{\widetilde{v\cdot F}(0)\oplus v\cdot b}$. Since the sum $\sum_{v\in\mathbb{F}_2^{n*}} (-1)^{\widetilde{v\cdot F}(0)\oplus v\cdot b}$ has an odd value ($\mathbb{F}_2^{n*}$ having an odd size), we deduce that, if $m \leq n$ then $2^{n/2-m}$ must be an integer. And it is also easily shown that $m > n$ is impossible. Hence:

Proposition 4 *Bent (n, m)-functions exist only if n is even and $m \leq n/2$.*

We shall see below that, for every ordered pair (n, m) satisfying this condition, bent functions do exist.

Open problem: Find a better bound than the covering radius bound for:
- n odd and $m < n$ (we shall see that for $m \geq n$, the Sidelnikov-Chabaud-Vaudenay bound, and other bounds if m is large enough, are better);
- n even and $n/2 < m < n$ (idem).

Primary constructions of bent functions: The two main classes of bent Boolean functions described in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" lead to two classes of bent (n, m)-functions (this was first observed by Nyberg in [135]). 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 $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$.

• Let us define $F(x,y)=L(x\,\pi(y))+H(y)$, where the product $x\,\pi(y)$ is calculated in $\mathbb{F}_{2^{n/2}}$, where L is any linear or affine mapping from $\mathbb{F}_{2^{n/2}}$ onto $\mathbb{F}_2^m$, π is any permutation of $\mathbb{F}_{2^{n/2}}$ and H is any $(n/2,m)$-function. This gives a bent function that we shall call *strict Maiorana-McFarland's bent* (n,m)-function. More generally, we obtain bent functions (that we can call *general Maiorana-McFarland's bent* (n,m)-functions) by taking for $F=(f_1,\cdots,f_m)$ any (n,m)-function such that, for every $v\in\mathbb{F}_2^{m*}$, the Boolean function $v\cdot F=v_1f_1\oplus\cdots\oplus v_mf_m$ belongs, up to linear equivalence, to the original Maiorana-McFarland class of bent functions. The function $L(x\,\pi(y))+H(y)$ has this property, since the function $v\cdot L(z)$ being a nonzero linear function, it equals $tr_{\frac{n}{2}}(\lambda\, z)$ for some $\lambda\neq 0$, where $tr_{\frac{n}{2}}(x)=x+x^2+x^{2^2}+\cdots+x^{2^{\frac{n}{2}-1}}$ is the (absolute) trace function from $\mathbb{F}_{2^{n/2}}$ to $\mathbb{F}_2$.

An example of general Maiorana-McFarland's bent function is given in [147]: the i-th coordinate of this function is defined as $f_i(x,y)=tr_{\frac{n}{2}}(x\,\phi_i(y))\oplus g_i(y)$, $x,y\in\mathbb{F}_{2^{n/2}}$, where g_i is any Boolean function on $\mathbb{F}_{2^{n/2}}$ and where $\phi_i(y)=\begin{cases}0 \text{ if } y=0\\ \alpha^{dec(y)+i-1} \text{ otherwise}\end{cases}$, where α is 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 in fact to the strict Maiorana-McFarland class of bent functions because the mapping $y\rightarrow\begin{cases}0 \text{ if } y=0\\ \alpha^{dec(y)} \text{ otherwise}\end{cases}$ is a permutation from $\mathbb{F}_2^{n/2}$ to $\mathbb{F}_{2^{n/2}}$, and the function $L:x\in\mathbb{F}_{2^{n/2}}\rightarrow(tr_{\frac{n}{2}}(x),tr_{\frac{n}{2}}(\alpha x),\cdots,tr_{\frac{n}{2}}(\alpha^{n/2-1}x))\in\mathbb{F}_2^{n/2}$ is an isomorphism.
Examples of functions in the general class which may not all belong to the strict class are the bent quadratic functions (*i.e.* the bent functions of algebraic degree 2).
Modifications of the Maiorana-McFarland bent functions have been proposed in [138], using the classes $\mathcal{C}$ and $\mathcal{D}$ of bent Boolean functions recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes".

• Defining $F(x,y)=G(xy^{2^n-2})=G(\frac{x}{y})$ (with $\frac{x}{y}=0$ if $y=0$), where G is a balanced $(n/2,m)$-function, gives also a bent (n,m)-function: for every $v\neq 0$, the function $v\cdot F$ belongs to the class $\mathcal{PS}_{ap}$ of Dillon's functions (seen in the chapter "Boolean Functions for Cryptography and Error Correcting Codes"), according to Proposition 2.

Remark. The functions above are given as defined over $\mathbb{F}_{2^{n/2}}\times\mathbb{F}_{2^{n/2}}$. In the case they are valued in $\mathbb{F}_{2^{n/2}}$, we may want to see them as functions from $\mathbb{F}_{2^n}$ to itself and wish to express them in the univariate representation. If $n/2$ is odd, this is quite easy: we have then $\mathbb{F}_{2^{n/2}} \cap \mathbb{F}_4 = \mathbb{F}_2$ and we can choose the basis $(1, w)$ of the 2-dimensional vector space $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^{n/2}}$, where w is a primitive element of $\mathbb{F}_4$. Then $w^2 = w + 1$ and $w^{2^{n/2}} = w^2$ since $n/2$ is odd. A general element of $\mathbb{F}_{2^n}$ has the form $X = x + wy$ where $x, y \in \mathbb{F}_{2^{n/2}}$ and we have $X^{2^{n/2}} = x + w^2 y = X + y$ and therefore $y = X + X^{2^{n/2}}$, and $x = w^2 X + wX^{2^{n/2}}$. For instance, the univariate representation of the simplest Maiorana-McFarland function, that is the function $(x, y) \to xy$, is $(X + X^{2^{n/2}})(w^2 X + wX^{2^{n/2}})$, that is, up to linear terms: $X^{1+2^{n/2}}$.

• We have already observed that constructing a bent (n, m)-function corresponds to finding an m-dimensional vectorspace of functions whose nonzero elements are all bent. An example (found by the author in common with G. Leander) of such construction is the following: let n be divisible by 2 but not by 4. Then $\mathbb{F}_{2^{n/2}}$ consists of cubes only (since $gcd(3, 2^{n/2} - 1) = 1$). If we choose some $w \in \mathbb{F}_{2^n}$ which is not a cube, then all the nonzero elements of the vector space $U = w\,\mathbb{F}_{2^{n/2}}$ are non-cubes. Then if $F(X) = X^d$ where $d = 2^i + 1$ (d is called a Gold exponent, see below) or $2^{2i} - 2^i + 1$ (d is then called a Kasami exponent) and $gcd(n, i) = 1$, all the functions $tr_n(vF(X))$, where $v \in U^*$, are bent (see the section on bent functions in the chapter "Boolean Functions for Cryptography and Error Correcting Codes"). This leads to the bent $(n, n/2)$-functions $X \in \mathbb{F}_{2^n} \to (tr_n(\beta_1 wX^d), \cdots, tr_n(\beta_{n/2} wX^d) \in \mathbb{F}_2^{n/2}$, where $(\beta_1, \cdots, \beta_{n/2})$ is a basis of $\mathbb{F}_{2^{n/2}}$ over $\mathbb{F}_2$. Let us see how these functions can be represented as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{n/2}}$. Let us choose a basis $(\alpha_1, \cdots, \alpha_{n/2})$ of $\mathbb{F}_{2^{n/2}}$ orthogonal to $(\beta_1, \cdots, \beta_{n/2})$, that is, such that $tr_{\frac{n}{2}}(\alpha_i \beta_j) = \delta_{i,j}$. Since the two bases are orthogonal, for every $y \in \mathbb{F}_{2^{n/2}}$, we have $y = \sum_{j=1}^{n/2} \alpha_j tr_{\frac{n}{2}}(\beta_j y)$. For every $X \in \mathbb{F}_{2^n}$, the image of X by the function equals $\sum_{j=1}^{n/2} \alpha_j tr_n(\beta_j wX^d) = \sum_{j=1}^{n/2} \alpha_j tr_{\frac{n}{2}}(\beta_j (wX^d + (wX^d)^{2^{n/2}})) = wX^d + (wX^d)^{2^{n/2}}$. Let us see now how, in the case of the Gold exponent, it can be represented as a function from $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ to $\mathbb{F}_{2^{n/2}}$: we express X in the form $x + wy$ where $x, y \in \mathbb{F}_{2^{n/2}}$ and if n is not a multiple of 3, we can take for w a primitive element of $\mathbb{F}_4$ (otherwise, all elements of F_4 are cubes and we have then to take w outside F_4), for which we have then $w^2 = w + 1$, $w^{2^i} = w^2$ (since i is necessarily odd) and $w^{2^i+1} = w^3 = 1$. We have then $X^d = x^{2^i+1} + wx^{2^i} y + w^2 xy^{2^i} + y^{2^i+1}$ and $wX^d + (wX^d)^{2^{n/2}} = (w + w^2)x^{2^i+1} + (w^2 + w)x^{2^i} y + (w^3 + w^3)xy^{2^i} + (w + w^2)y^{2^i+1} = x^{2^i+1} + x^{2^i} y + y^{2^i+1}$.
It would be nice being able to do the same for the Kasami function.

Note that, in the case of the Gold functions x^d with $d = 2^i + 1$, we can extend the construction to the case where i is not co-prime with n. The exact condition for $tr_n(vX^d)$ to be bent is then (as we saw in the chapter "Boolean Functions for Cryptography and Error Correcting Codes") that $\frac{n}{gcd(i,n)}$ is even and $v \notin \{x^d,\, x \in \mathbb{F}_{2^n}\}$.

A class of bent vectorial functions can be found in [92] and a survey on the subject can be found in [61].

Secondary constructions: Given any bent (n, m)-function F, any chopped function obtained by deleting some coordinates of F (or more generally by composing it on the left with any surjective affine mapping) is obviously still bent. But there exist other more useful secondary constructions (that is, constructions of new bent functions from known ones). In [50] is given the following secondary construction of bent Boolean functions (recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes"): 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 mapping 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 $f_{\phi,g}(x, y) = x \cdot \phi(y) \oplus g(y)$, $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^s$, 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 5 *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) mapping 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 $\mathbb{F}_{2^r}$.*

Indeed, taking $x \cdot y = tr_r(xy)$ for inner product in $\mathbb{F}_{2^r}$, for every $v \in \mathbb{F}_{2^r}^*$, the function $tr_r(v\,F_{\psi,H}(x, y))$ is bent, according to the result of [50] recalled above, with $\phi(y) = v\,\psi(y)$ and $g(y) = tr_r(v\,H(y))$. 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, according to Proposition 4, for allowing the restrictions of H to be bent. The condition on ψ being easily satisfied[9], it is then a simple matter to choose

[9] Note that it does not make ψ necessarily affine.

H. Hence, this construction is quite effective (but only for designing bent (n,m)-functions such that $m \leq n/4$, since $r \leq \frac{s}{3}$ is equivalent to $r \leq \frac{r+s}{4}$).

In [49] is given another secondary construction of bent Boolean functions, which is very general and can be adapted to vectorial functions as follows:

Proposition 6 *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 $H_y : x \in \mathbb{F}_2^r \to H(x,y)$ 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 $\sum_{x\in\mathbb{F}_2^r}(-1)^{v\cdot H(x,y)\oplus a\cdot x} = 2^{r/2}(-1)^{f_{a,v}(y)}$. 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.*

Indeed, we have, for every nonzero $v \in \mathbb{F}_2^m$ and every $a \in \mathbb{F}_2^r$ and $b \in \mathbb{F}_2^s$:

$$\sum_{\substack{x\in\mathbb{F}_2^r \\ y\in\mathbb{F}_2^s}} (-1)^{v\cdot H(x,y)\oplus a\cdot x\oplus b\cdot y} = 2^{r/2} \sum_{y\in\mathbb{F}_2^s} (-1)^{f_{a,v}(y)\oplus b\cdot y}.$$

An example of application of Proposition 6 is when we choose every H_y in the Maiorana-McFarland's 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 $y \in \mathbb{F}_2^s$. According to the results recalled in the previous chapter on the duals of Maiorana-McFarland's functions, for every $v \in \mathbb{F}_{2^{r/2}}^*$ and every $a, a' \in \mathbb{F}_{2^{r/2}}$, we have then $f_{(a,a'),v}(y) = tr_{\frac{r}{2}}\left(a'\,\pi_y^{-1}\left(\frac{a}{v}\right) + v\,G_y\left(\pi_y^{-1}\left(\frac{a}{v}\right)\right)\right)$, where $tr_{\frac{r}{2}}$ is the trace function from $\mathbb{F}_{2^{r/2}}$ to $\mathbb{F}_2$. 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 $y \to tr_{\frac{r}{2}}\left(a'\,\pi_y^{-1}(a) + v\,G_y(\pi_y^{-1}(a))\right)$ 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 mapping $y \to \pi_y^{-1}(a)$ 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 $y \to G_y(a)$ is bent.

An obvious corollary of Proposition 6 is that the so-called *direct sum of bent functions* gives bent functions: we define $H(x,y) = F(x) + G(y)$, where F is any bent (r,m)-function and G any bent (s,m)-function, and we have then $f_{a,v}(y) = \widetilde{v\cdot F}(a) \oplus v \cdot G(y)$, which is a bent Boolean function for every a and every $v \neq 0$. Hence, H is bent.

Remark. The direct sum of bent Boolean functions has been generalized into the indirect sum (see the previous chapter). The direct sum of bent vectorial functions cannot be similarly generalized into a secondary construction of bent vectorial functions, as is. As mentioned in [51], we can identify $\mathbb{F}_2^m$ with $\mathbb{F}_{2^m}$ and define $H(x,y) = F_1(x) + G_1(y) + (F_1(x) + F_2(x))\,(G_1(y)+G_2(y))$, where F_1 and F_2 are (r,m)-functions and G_1 and G_2 are (s,m)-functions. However, in general, Proposition 6 cannot be applied as is. Indeed, taking (as usual) for inner product in $\mathbb{F}_{2^m}$: $u \cdot v = tr_m(uv)$, then $v \cdot H_y(x)$ equals:

$$tr_m(v\,F_1(x)) \oplus tr_m(v\,G_1(y)) + tr_m\left(v\,(F_1(x) + F_2(x))\,(G_1(y) + G_2(y))\right),$$

which does not enter, in general, in the framework of the construction of Boolean functions called "indirect sum". Note that the function $f_{a,v}$ exists under the sufficient condition that, for every nonzero ordered pair $(v,w) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, the function $tr_m(v\,F_1(x)) + tr_m(w\,F_2(x))$ is bent (which is equivalent to saying that the $(r,2m)$-function (F_1,F_2) is bent). There are particular cases where the construction works.

Open problem: Find new constructions of bent (perfect nonlinear) functions.

3.1.2 The Sidelnikov-Chabaud-Vaudenay bound

Since bent (n,m)-functions do not exist if $m > n/2$, this leads to asking the question whether better upper bounds than the covering radius bound can be proved in this case. Such bound has been (in a way) re-discovered[10] by Chabaud and Vaudenay in [65]:

Theorem 1 *Let n and m be any positive integers such that $m \geq n-1$. Let F be any (n,m)-function. Then:*

$$nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

Proof. Recall that $nl(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_2^{m\,*};\; u \in \mathbb{F}_2^n} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right|$. We have:

$$\max_{\substack{v \in \mathbb{F}_2^{m\,*}\\ u \in \mathbb{F}_2^n}} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right)^2 \geq \frac{\sum_{\substack{v \in \mathbb{F}_2^{m\,*}\\ u \in \mathbb{F}_2^n}} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right)^4}{\sum_{\substack{v \in \mathbb{F}_2^{m\,*}\\ u \in \mathbb{F}_2^n}} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x} \right)^2}. \quad (8)$$

[10] We write "re-discovered" because a bound on sequences due to Sidelnikov [150] is equivalent to the bound obtained by Chabaud and Vaudenay for power functions and its proof is in fact valid for all functions.

Parseval's relation (see the previous chapter) states that, for every $v \in \mathbb{F}_2^m$:

$$\sum_{u\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 = 2^{2n}. \tag{9}$$

Using the fact (already used in the proof of Proposition 2) that any character sum $\sum_{x\in E}(-1)^{\ell(x)}$ associated to a linear function ℓ over any $\mathbb{F}_2$-vectorspace E is nonzero if and only if ℓ is null on E, we have:

$$\begin{aligned}
& \sum_{v\in\mathbb{F}_2^m,\ u\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^4 \\
= \ & \sum_{x,y,z,t\in\mathbb{F}_2^n}\left[\sum_{v\in\mathbb{F}_2^m}(-1)^{v\cdot(F(x)+F(y)+F(z)+F(t))}\right]\left[\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot(x+y+z+t)}\right] \\
= \ & 2^{n+m}\left|\left\{(x,y,z,t)\in\mathbb{F}_2^{4n}/\left\{\begin{array}{ll} x+y+z+t & =0 \\ F(x)+F(y)+F(z)+F(t) & =0\end{array}\right.\right\}\right| \\
= \ & 2^{n+m}|\{(x,y,z)\in\mathbb{F}_2^{3n}/\,F(x)+F(y)+F(z)+F(x+y+z)=0\}| \qquad (10) \\
\geq \ & 2^{n+m}|\{(x,y,z)\in\mathbb{F}_2^{3n}/\,x=y \text{ or } x=z \text{ or } y=z\}|. \qquad (11)
\end{aligned}$$

Clearly: $|\{(x,y,z)/\,x=y \text{ or } x=z \text{ or } y=z\}| = 3\cdot|\{(x,x,y)/\,x,y\in\mathbb{F}_2^n\}| - 2\cdot|\{(x,x,x)/\,x\in\mathbb{F}_2^n\}| = 3\cdot 2^{2n}-2\cdot 2^n$. Hence, according to Relation (8):

$$\max_{v\in\mathbb{F}_2^{m*};\ u\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 \geq$$

$$\frac{2^{n+m}(3\cdot 2^{2n}-2\cdot 2^n)-2^{4n}}{(2^m-1)\,2^{2n}} = 3\times 2^n-2-2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}$$

and this gives the desired bound, according to Relation (6). □

The condition $m \geq n-1$ is assumed in Theorem 1 to make non-negative the expression located under the square root. Note that for $m = n-1$, this *Sidelnikov-Chabaud-Vaudenay bound* coincides with the covering radius bound. For $m \geq n$, it strictly improves upon it. For $m > n$, the square root in it cannot be an integer (see [65]). Hence, the Sidelnikov-Chabaud-Vaudenay bound can be tight only if $n = m$ with n odd. We shall see in the next subsection that, under this condition, it is actually tight.

Other bounds have been obtained in [58] and improve, when m is sufficiently greater than n (which makes them less interesting, cryptographically), upon the covering radius bound and the Sidelnikov-Chabaud-Vaudenay bound (examples are given).

3.1.3 Almost bent and almost perfect nonlinear functions

Almost bent functions

Definition 7 *[65] The (n, n)-functions F which achieve the bound of Theorem 1 with equality – that is, such that $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$ (n odd)– are called* almost bent *(AB).*

Remark. The term of *almost* bent is a little misleading. It gives the feeling that these functions are not quite optimal. But they are. Recall that, according to Nyberg's result (Proposition 4), (n, n)-bent functions do not exist.

According to Inequality (8), the AB functions are those (n, n)-functions such that, for every $u, v \in \mathbb{F}_2^n$, $v \neq 0$, the sum $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x} = \widehat{1_{G_F}}(u, v)$ equals 0 or $\pm 2^{\frac{n+1}{2}}$ (indeed, the maximum of a sequence of nonnegative integers equals the ratio of the sum of their squares over the sum of their values if and only if these integers take at most one nonzero value). Note that this condition does not depend on the choice of the inner product.

There exists a bound on the algebraic degree of AB functions, similar to the bound for bent functions:

Proposition 7 *[56] Let F be any (n, n)-function ($n \geq 3$). If F is AB, then the algebraic degree of F is less than or equal to $(n + 1)/2$.*

This is a direct consequence of the fact that the Walsh transform of any function $v \cdot F$ is divisible by $2^{\frac{n+1}{2}}$ and the fact, recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", that if the Walsh transform values of an n-variable Boolean function are divisible by 2^k, then the algebraic degree of the function is at most $n - k + 1$. Note that the divisibility plays also a role with respect to the algebraic degree of the composition of two vectorial functions: in [48] has been proved that, if the Walsh transform values of a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are divisible by 2^ℓ then, for every vectorial function $F' : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the algebraic degree of $F' \circ F$ is at most equal to the algebraic degree of F' plus $n - \ell$. This means that using AB power functions as S-boxes in block ciphers may not be a good idea. Suboptimal functions (as the multiplicative inverse function, see below) may be better (as usual in cryptography).

Almost perfect nonlinear functions Inequality (11) is an equality if and only if the relation $F(x)+F(y)+F(z)+F(x+y+z)=0$ can be achieved only when $x=y$ or $x=z$ or $y=z$. There are several equivalent ways of characterizing this property:
- the restriction of F to any 2-dimensional flat (*i.e.* affine subspace) of $\mathbb{F}_2^n$ is non-affine (indeed, the set $\{x,y,z,x+y+z\}$ is a flat and it is 2-dimensional if and only if $x\neq y$ and $x\neq z$ and $y\neq z$; saying that $F(x)+F(y)+F(z)+F(x+y+z)=0$ is equivalent to saying that the restriction of F to this flat is affine, since we know that a function F is affine on a flat A if and only if, for every x,y,z in A we have $F(x+y+z)=F(x)+F(y)+F(z)$);
- for every distinct nonzero (that is, $\mathbb{F}_2$-linearly independent) vectors a and a', the second order derivative $D_aD_{a'}F(x)=F(x)+F(x+a)+F(x+a')+F(x+a+a')$ takes only non-zero values;
- the equation $F(x)+F(x+a)=F(y)+F(y+a)$ (obtained from $F(x)+F(y)+F(z)+F(x+y+z)=0$ by denoting $x+z$ by a) can be achieved only for $a=0$ or $x=y$ or $x=y+a$;
- for every $a\in\mathbb{F}_2^{n*}$ and every $b\in\mathbb{F}_2^n$, the equation $F(x)+F(x+a)=b$ has at most 2 solutions (that is, 0 or 2 solutions, since if it has one solution x, then it has $x+a$ for second solution).

Definition 8 *[142, 8, 137] An (n,n)-function F is called* almost perfect nonlinear *(APN) if, for every $a\in\mathbb{F}_2^{n*}$ and every $b\in\mathbb{F}_2^n$, the equation $F(x)+F(x+a)=b$ has 0 or 2 solutions; that is, equivalently, if the restriction of F to any 2-dimensional flat (*i.e. *affine subspace) of $\mathbb{F}_2^n$ is non-affine.*

Remark. Here again, the term of *almost* perfect nonlinear is a little misleading, giving the feeling that these functions are almost optimal while they are optimal.

According to the proof of Sidelnikov-Chabaud-Vaudenay's bound above, every AB function is APN (this was first observed by Chabaud and Vaudenay). In fact, this implication can be more precisely changed into a characterization of AB functions (see Proposition 8 below), involving the notion of plateaued function.

Definition 9 *An (n,m)-function is called* plateaued *if, for every nonzero $v\in\mathbb{F}_2^m$, the component function $v\cdot F$ is plateaued, that is, there exists a positive integer λ_v (called the amplitude of the plateaued Boolean function*

$v \cdot F$) such that the values of its Walsh transform: $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$, $u \in \mathbb{F}_2^n$, all belong to the set $\{0, \pm\lambda_v\}$.

Then, because of Parseval's relation (9), 2^{2n} equals λ_v^2 times the size of the set $\{u \in \mathbb{F}_2^n \,/\, \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x} \neq 0\}$, and λ_v equals then a power of 2 whose exponent is greater than or equal to $n/2$ (since this size is at most 2^n). The extreme case $\lambda_v = 2^{n/2}$ corresponds to the case where $v \cdot F$ is bent. Every *quadratic* function (that is, every function of algebraic degree 2) is plateaued, see the chapter "Boolean Functions for Cryptography and Error Correcting Codes".
It has been proved in [36] that no power plateaued bijective (n, n)-function exists[11] when n is a power of 2 and in [132] that no such function exists with Walsh spectrum $\{0, \pm 2^{n/2+1}\}$ when n is divisible by 4.

Proposition 8 *Every AB function is APN. More precisely, any vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is AB if and only if F is APN and the functions $v \cdot F$, $v \neq 0$, are plateaued with the same amplitude.*

This comes directly from Relations (8) and (11). *We shall see below, in Proposition 15, that if n is odd, the condition "with the same amplitude" is in fact not necessary.*
Note that, according to Relations (10) and (11), and to the two lines following them, APN (n, n)-functions F are characterized by the fact that the power sums of degree 4 of the values of their Walsh transform take the minimal value $3 \cdot 2^{4n} - 2 \cdot 2^{3n}$, that is, F is APN if and only if:

$$\sum_{v\in\mathbb{F}_2^n, u\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^4 = 3 \cdot 2^{4n} - 2 \cdot 2^{3n} \qquad (12)$$

or equivalently, replacing $\sum_{u\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot x}\right)^4$ by its value 2^{4n} and using Parseval's relation (9):

Proposition 9 *Any (n, n)-function F is APN if and only if*

$$\sum_{\substack{v\in\mathbb{F}_2^{n*}\\ u\in\mathbb{F}_2^n}} \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 \left(\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 - 2^{n+1}\right) = 0. \quad (13)$$

[11] A conjecture by T. Helleseth states that there is no power permutation having 3 Walsh transform values when n is a power of 2.

This characterization will have nice consequences in the sequel.
Note that, similarly as for the power sum of degree 4, the power sum $\sum_{v\in\mathbb{F}_2^n,u\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^3$ of degree 3 equals

$$2^{2n}\left|\left\{(x,y)\in\mathbb{F}_2^{2n}/\,F(x)+F(y)+F(x+y)=0\right\}\right|.$$

Applying (with $z=0$) the property that, for every APN function F, the relation $F(x)+F(y)+F(z)+F(x+y+z)=0$ can be achieved only when $x=y$ or $x=z$ or $y=z$, we have then, for every APN function such that $F(0)=0$:

$$\sum_{v\in\mathbb{F}_2^n,u\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^3=3\cdot 2^{3n}-2\cdot 2^{2n}. \qquad (14)$$

But this property is not characteristic (except for quadratic functions, see below) of APN functions among those (n,n)-functions such that $F(0)=0$, since it is only characteristic of the fact that $\sum_{x\in E}F(x)\neq 0$ for every 2-dimensional vector subspace E of $\mathbb{F}_2^n$.

APN property is a particular case of a notion introduced by Nyberg [135, 136]: an (n,m)-function F is called *differentially δ-uniform* if, for every nonzero $a\in\mathbb{F}_2^n$ and every $b\in\mathbb{F}_2^m$, the equation $F(x)+F(x+a)=b$ has at most δ solutions. The number δ is then bounded below by 2^{n-m} and equals 2^{n-m} if and only if F is perfect nonlinear. The behavior of δ for general S-boxes has been studied in [155].
The smaller δ is, the better is the contribution of F to a resistance to differential cryptanalysis. When $m=n$, the smallest possible value of δ is 2, since we already saw that if x is a solution of equation $F(x)+F(x+a)=b$ then $x+a$ is also a solution. Hence, APN functions contribute to a maximal resistance to differential cryptanalysis when $m=n$ and AB functions contribute to a maximal resistance to both linear and differential cryptanalyses.

Note that if F is a quadratic (n,n)-function, the equation $F(x)+F(x+a)=b$ is a linear equation. It admits then at most 2 solutions for every nonzero a and every b if and only if the related homogeneous equation $F(x)+F(x+a)+F(0)+F(a)=0$ admits at most 2 solutions for every nonzero a. Hence, F is APN if and only if the associated bilinear symmetric $(2n,n)$-function $\varphi_F(x,y)=F(0)+F(x)+F(y)+F(x+y)$ never vanishes when x and y are $\mathbb{F}_2$-linearly independent vectors of $\mathbb{F}_2^n$. For functions of higher degrees, the fact that $\varphi_F(x,y)$ (which is no longer bilinear) never vanishes when x and y are linearly independent is only a necessary condition for APNness.

A subclass of APN functions (and a potential superclass of APN quadratic permutations), called crooked functions, has been considered in [6] and further studied in [35, 76, 120]. All known crooked functions are quadratic. It can be proved [121] that every power crooked function is a Gold function (see definition below).

Other characterizations of AB and APN functions

• A necessary condition dealing with *quadratic terms in the ANF of any APN function* has been observed in [8]. Given any APN function F (quadratic or not), every quadratic term x_ix_j ($1 \leq i < j \leq n$) must appear with a non-null coefficient in the algebraic normal form of F. Indeed, we know that the coefficient of any monomial $\prod_{i\in I} x^i$ in the ANF of F equals $a_I = \sum_{x\in\mathbb{F}_2^n/\ supp(x)\subseteq I} F(x)$ (this sum being calculated in $\mathbb{F}_2^n$). Applied for instance to $I = \{n-1, n\}$, this gives $a_I = F(0,\ldots,0,0,0) + F(0,\ldots,0,0,1) + F(0,\ldots,0,1,0) + F(0,\ldots,0,1,1)$, and F being APN, this vector can not be null. Note that, since the notion of almost perfect nonlinearity is affinely invariant (see below), this condition must be satisfied by all of the functions $L' \circ F \circ L$, where L' and L are affine automorphisms of $\mathbb{F}_2^n$. Extended this way, the condition becomes necessary and sufficient (indeed, for every distinct x, y, z in $\mathbb{F}_2^n$, there exists an affine automorphism L of $\mathbb{F}_2^n$ such that $L(0,\ldots,0,0,0) = x$, $L(0,\ldots,0,1,0) = y$ and $L(0,\ldots,0,0,1) = z$).

• The properties of APNness and ABness can be translated in terms of Boolean functions, as observed in [56]:

Proposition 10 *Let F be any (n,n)-function. For every $a, b \in \mathbb{F}_2^n$, let $\gamma_F(a,b)$ equal 1 if the equation $F(x) + F(x+a) = b$ admits solutions, with $a \neq 0$. Otherwise, let $\gamma_F(a,b)$ be null. Then, F is APN if and only if γ_F has weight $2^{2n-1} - 2^{n-1}$, and F is AB if and only if γ_F is bent. The dual of γ_F is then the indicator of the Walsh support of F, deprived of* $(0,0)$.

Proof.
1) If F is APN, then for every $a \neq 0$, the mapping $x \mapsto F(x) + F(x+a)$ is two-to-one (that is, the size of the pre-image of any vector equals 0 or 2). Hence, γ_F has weight $2^{2n-1} - 2^{n-1}$. The converse is also straightforward.
2) We assume now that F is APN. For every $u, v \in \mathbb{F}_2^n$, replacing $(-1)^{\gamma_F(a,b)}$

by $1-2\gamma_F(a,b)$ in the character sum $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{\gamma_F(a,b)\oplus u\cdot a\oplus v\cdot b}$ leads to $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{u\cdot a\oplus v\cdot b}-2\sum_{a,b\in\mathbb{F}_2^n}\gamma_F(a,b)(-1)^{u\cdot a\oplus v\cdot b}$. Denoting by δ_0 the Dirac symbol ($\delta_0(u,v)=1$ if $u=v=0$ and 0 otherwise), we deduce that the Walsh transform of γ_F equals $2^{2n}\ \delta_0(u,v)-\sum_{x\in\mathbb{F}_2^n,a\in\mathbb{F}_2^{n*}}(-1)^{u\cdot a\oplus v\cdot(F(x)+F(x+a))}=2^{2n}\ \delta_0(u,v)-\left(\sum_{x,y\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus v\cdot F(y)\oplus u\cdot x\oplus u\cdot y}\right)+2^n=2^{2n}\ \delta_0(u,v)-\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2+2^n$. Hence, F is AB if and only if the value of this Walsh transform equals $\pm 2^n$ at every $(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^n$, *i.e.* if γ_F is bent. Moreover, if γ_F is bent, then for every $(u,v)\neq 0$, we have $\widetilde{\gamma_F}(u,v)=0$, that is, $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{\gamma_F(a,b)\oplus u\cdot a\oplus v\cdot b}=2^n$ if and only if $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}=0$. Hence, the dual of γ_F is the indicator of the Walsh support of F, deprived of $(0,0)$. □

• Obviously, an (n,n)-function F is APN if and only if, for every $(a,b)\neq(0,0)$, the system $\begin{cases} x+y &= a\\ F(x)+F(y) &= b\end{cases}$ admits 0 or 2 solutions. As shown by van Dam and Fon-Der-Flaass in [76], it is AB if and only if the system $\begin{cases} x+y+z &= a\\ F(x)+F(y)+F(z) &= b\end{cases}$ admits $3\cdot 2^n-2$ solutions if $b=F(a)$ and 2^n-2 solutions otherwise. This can easily be proved by using the facts that F is AB if and only if, for every $v\in\mathbb{F}_2^{n*}$ and every $u\in\mathbb{F}_2^n$, we have $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^3=2^{n+1}\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$, and that two pseudo-Boolean functions (that is, two functions from $\mathbb{F}_2^n$ to $\mathbb{Z}$) are equal to each other if and only if their discrete Fourier transforms are equal to each other: the value at (a,b) of the Fourier transform of the function of (u,v) equal to $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^3$ if $v\neq 0$, and to 0 otherwise equals

$$\sum_{\substack{u\in\mathbb{F}_2^n\\ v\in\mathbb{F}_2^n}}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^3(-1)^{a\cdot u\oplus b\cdot v}-2^{3n}=$$

$$2^{2n}\left|\left\{(x,y,z)\in\mathbb{F}_2^{3n}\ /\ \left\{\begin{array}{l} x+y+z=a\\ F(x)+F(y)+F(z)=b\end{array}\right.\right\}\right|-2^{3n},$$

and the value of the Fourier transform of the function which is equal to $2^{n+1}\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ if $v\neq 0$, and to 0 otherwise equals

$$2^{3n+1}\left|\left\{x\in\mathbb{F}_2^n\ /\ \left\{\begin{array}{l} x=a\\ F(x)=b\end{array}\right.\right\}\right|-2^{2n+1}.$$

This proves the result. Note that $3\cdot 2^n-2$ is the number of triples (x,x,a), (x,a,x) and (a,x,x) where x ranges over $\mathbb{F}_2^n$. Hence the condition when $F(a)=b$ means that these particular triples are the only solutions of the system $\left\{\begin{array}{lcl} x+y+z & = & a \\ F(x)+F(y)+F(z) & = & F(a) \end{array}\right.$. This is equivalent to saying that F is APN and we can therefore replace the first condition of van Dam and Fon-Der-Flaass by "F is APN". Denoting $c=F(a)+b$, we have then:

Proposition 11 *Let n be any positive integer and F any APN (n,n)-function. Then F is AB if and only if, for every $c\neq 0$ and every a in $\mathbb{F}_2^n$, the equation $F(x)+F(y)+F(a)+F(x+y+a)=c$ has 2^n-2 solutions.*

Let us denote by $\mathcal{A}_2$ the set of 2-dimensional flats of $\mathbb{F}_2^n$ and by Φ_F the mapping $A\in\mathcal{A}_2\rightarrow\sum_{x\in A}F(x)\in\mathbb{F}_2^n$. Proposition 11 is equivalent to saying that an APN function is AB if and only if, for every $a\in\mathbb{F}_2^n$, the restriction of Φ_F to those flats which contain a is a $\frac{2^{n-1}-1}{3}$-to-1 function. Hence we have:

Corollary 1 *Any (n,n)-function F is APN if and only if Φ_F is valued in $\mathbb{F}_2^{n*}=\mathbb{F}_2^n\setminus\{0\}$, and F is AB if and only if, additionally, the restriction of $\Phi_F:\mathcal{A}_2\rightarrow\mathbb{F}_2^{n*}$ to those flats which contain a vector a is a balanced function, for every $a\in\mathbb{F}_2^n$.*

Note that, for every APN function F and any two distinct vectors a and a', the restriction of Φ_F to those flats which contain a and a' is injective, since for two such distinct flats $A=\{a,a',x,x+a+a'\}$ and $A'=\{a,a',x',x'+a+a'\}$, we have $\Phi_F(A)+\Phi_F(A')=F(x)+F(x+a+a')+F(x')+F(x'+a+a')=\Phi_F(\{x,x+a+a',x',x'+a+a'\})\neq 0$. But this restriction of Φ_F cannot be surjective since the number of flats containing a and a' equals $2^{n-1}-1$, which is less than 2^n-1.

Remark: Other characterizations can be derived with the same method as in the proof of the result of van Dam and Fon-Der-Flaass. For instance, F is AB if and only if, for every $v\in\mathbb{F}_2^{n*}$ and every $u\in\mathbb{F}_2^n$, we have $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^4=2^{n+1}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2$. By applying again the Fourier transform and dividing by 2^{2n}, we deduce that F is AB if and only if, for every (a,b), we have

$$\left|\left\{(x,y,z,t)\in\mathbb{F}_2^{4n}/\left\{\begin{array}{l} x+y+z+t=a \\ F(x)+F(y)+F(z)+F(t)=b \end{array}\right.\right\}\right|-2^{2n}=$$

$$2^{n+1}\left|\left\{(x,y)\in\mathbb{F}_2^{2n} \,/\, \left\{\begin{array}{l} x+y=a \\ F(x)+F(y)=b \end{array}\right\}\right|-2^{n+1}.$$

Hence, F is AB if and only if the system $\left\{\begin{array}{lcl} x+y+z+t & = & a \\ F(x)+F(y)+F(z)+F(t) & = & b \end{array}\right.$ admits $3\cdot 2^{2n}-2^{n+1}$ solutions if $a=b=0$ (this is equivalent to saying that F is APN), $2^{2n}-2^{n+1}$ solutions if $a=0$ and $b\neq 0$ (note that this condition corresponds to adding all the conditions of Proposition 11 with c fixed to b and with a ranging over $\mathbb{F}_2^n$), and $2^{2n}+2^{n+2}\gamma_F(a,b)-2^{n+1}$ solutions if $a\neq 0$ (indeed, F is APN; note that this gives a new property of AB functions).

• A relationship has been observed in [56]) (see also [156, 58]) between the properties, for an (n,n)-function, of being APN or AB and properties of related codes:

Proposition 12 *Let F be any (n,n)-function such that $F(0)=0$. Let H be the matrix $\left[\begin{array}{ccccc} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{array}\right]$, where α is a primitive element of the field $\mathbb{F}_{2^n}$, and where each symbol stands for the column of its coordinates with respect to a basis of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_{2^n}$. Let C_F be the linear code admitting H for parity-check matrix. Then, F is APN if and only if C_F has minimum distance 5, and F is AB if and only if $C_F^\perp$ (*i.e.* the code admitting H for generator matrix) has weights $0, 2^{n-1}-2^{\frac{n-1}{2}}, 2^{n-1}$ and $2^{n-1}+2^{\frac{n-1}{2}}$.*

Proof. Since H contains no zero column, C_F has no codeword of Hamming weight 1 and since all columns of H are distinct vectors, C_F has no codeword of Hamming weight 2. Hence[12], C_F has minimum distance at least 3. This minimum distance is also at most 5 (this is known, see [56]). The fact that C_F has no codeword of weight 3 or 4 is by definition equivalent to the APNness of F, since a vector $(c_0, c_1, \cdots, c_{2^n-2})\in\mathbb{F}_2^{2^n-1}$ is a codeword if and only if $\left\{\begin{array}{l} \sum_{i=0}^{2^n-2} c_i\alpha^i=0 \\ \sum_{i=0}^{2^n-2} c_iF(\alpha^i)=0 \end{array}\right.$. The inexistence of codewords of weight 3 is then equivalent to the fact that $\sum_{x\in E}F(x)\neq 0$ for every 2-dimensional vector subspace E of $\mathbb{F}_{2^n}$ and the inexistence of codewords of weight 4 is equivalent to the fact that $\sum_{x\in A}F(x)\neq 0$ for every 2-dimensional flat A not containing 0. The characterization of ABness through the weights of $C_F^\perp$ comes directly from the characterization of AB functions by their Walsh

[12] We can also say that, C_F being a subcode of the Hamming code (see the definition of the Hamming code in the chapter "Boolean Functions for Cryptography and Error Correcting Codes"), it has minimum distance at least 3.

transform values, and from the fact that the weight of the Boolean function $v \cdot F(x) \oplus u \cdot x$ equals $2^{n-1} - \frac{1}{2}\widehat{1_{G_F}}(u,v)$. $\square$

Remark.
1. Any subcode of dimension $2^n - 1 - 2n$ of the $[2^n - 1, n, 3]$ Hamming code is a code C_F for some function F.
2. Proposition 12 assumes that $F(0) = 0$. If we want to express the APN-ness of any (n,n)-function, another matrix can be considered as in [23]: the $(2n+1) \times (2^n - 1)$ matrix $\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \\ F(0) & F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{bmatrix}$. Then F is APN if and only if the code $\widetilde{C_F}$ admitting this parity-check matrix has parameters $[2^n, 2^n - 1 - 2n, 6]$. To prove this, note first that this code does not change if we add a constant to F (contrary to C_F). Hence, by adding the constant $F(0)$, we can assume that $F(0) = 0$. Then, the code $\widetilde{C_F}$ is the extended code of C_F (obtained by adding to each codeword of C_F a first coordinate equal to the sum modulo 2 of its coordinates). Since $F(0) = 0$, we can apply Proposition 12 and it is clear that C_F is a $[2^n - 1, 2^n - 1 - 2n, 5]$ code if and only if $\widetilde{C_F}$ is a $[2^n, 2^n - 1 - 2n, 6]$ code (we know that C_F cannot have minimum distance greater than 5, as recalled in [56]).

As shown in [56], using Parseval's relation and Relations (12) and (14), it can be proved that the weight distribution of $C_F^\perp$ is unique[13] for every AB (n,n)-function F such that $F(0) = 0$: there are 1 codeword of null weight, $(2^n - 1)(2^{n-2} + 2^{\frac{n-3}{2}})$ codewords of weight $2^{n-1} - 2^{\frac{n-1}{2}}$, $(2^n - 1)(2^{n-2} - 2^{\frac{n-3}{2}})$ codewords of weight $2^{n-1} + 2^{\frac{n-1}{2}}$, and $(2^n - 1)(2^{n-1} + 1)$ codewords of weight 2^{n-1}. We shall see that the function $x \to x^3$ over the field $\mathbb{F}_{2^n}$ is an AB function. The code $C_F^\perp$ corresponding to this function is known in coding theory as the dual of the 2-error-correcting BCH code of length $2^n - 1$.

If F is APN on $\mathbb{F}_{2^n}$ and null at 0, and $n > 2$, it can also be proved that the code $C_F^\perp$ has dimension $2n$. Equivalently, let us prove that the code whose generator matrix equals $\begin{bmatrix} F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{bmatrix}$, and which

[13] Being able to determine such weight distribution is rare (when the code does not contain the all-one vector): it is equivalent to determining the Walsh value distribution of the function, and we have seen in the previous chapter that this is much more difficult in general than just determining the distribution of the absolute values, which for an AB function is easily deduced from the single Parseval's relation.

can therefore be seen as the code $\{tr_n(vF(x);\ v \in \mathbb{F}_{2^n}\}$, has dimension n and intersects the simplex code $\{tr_n(ux);\ u \in \mathbb{F}_{2^n}\}$ (whose generator matrix is equal to $\left[\begin{array}{ccccc} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \end{array}\right]$) only in the null vector. Slightly more generally:

Proposition 13 *Let F be an APN function in $n > 2$ variables. Then the nonlinearity of F cannot be null and, assuming that $F(0) = 0$, the code $C_F^\perp$ has dimension $2n$.*

Proof. Suppose there exists $v \neq 0$ such that $v \cdot F$ is affine. Without loss of generality (by composing F with an appropriate linear automorphism and adding an affine function to F), we can assume that $v = (0, \cdots, 0, 1)$ and that $v \cdot F$ is null. Then, every derivative of F is 2-to-1 and has null last coordinate. Hence, for every $a \neq 0$ and every b, the equation $D_aF(x) = b$ has no solution if $b_n = 1$ and it has 2 solutions if $b_n = 0$. The $(n, n-1)$ function obtained by erasing the last coordinate of $F(x)$ has therefore balanced derivatives; hence it is a bent $(n, n-1)$-function, a contradiction with Nyberg's result, since $n - 1 > n/2$. □

Note that for $n = 2$, the nonlinearity can be null. An example is the function $(x_1, x_2) \to (x_1x_2, 0)$.

J. Dillon (private communication) observed that the property of Proposition 13 implies that, for every nonzero $c \in \mathbb{F}_{2^n}$, the equation $F(x) + F(y) + F(z) + F(x + y + z) = c$ must have a solution (that is, the function Φ_F introduced after Proposition 11 is onto $\mathbb{F}_2^{n*}$). Indeed, otherwise, for every Boolean function $g(x)$, the function $F(x) + g(x)\,c$ would be APN. But this is contradictory with Proposition 13 if we take $g(x) = v_0 \cdot F(x)$ (that is, $g(x) = tr_n(v_0F(x))$ if we have identified $\mathbb{F}_2^n$ with the field $\mathbb{F}_{2^n}$) with $v_0 \notin c^\perp$, since we have then $v_0 \cdot [F(x) + g(x)\,c] = v_0 \cdot F(x) \oplus g(x)\,(v_0 \cdot c) = 0$.

There is a connection between AB functions and the so called *uniformly packed codes* [3]:

Definition 10 *Let C be any binary code of length N, with minimum distance $d = 2e + 1$ and covering radius ρ. For any $x \in \mathbb{F}_2^N$, let us denote by $\zeta_j(x)$ the number of codewords of C at distance j from x. The code C is called uniformly packed, if there exist real numbers h_0, h_1, ..., h_ρ such that, for any $x \in \mathbb{F}_2^N$, the following equality holds*

$$\sum_{j=0}^{\rho} h_j\ \zeta_j(x) = 1.$$

As shown in [4], this is equivalent to saying that the covering radius of the code equals its external distance (*i.e.* the number of different nonzero distances between the codewords of its dual). Then, as shown in [56]:

Proposition 14 *Let F be any polynomial of the form (3), where n is odd. Then F is AB if and only if C_F is a uniformly packed code of length $N = 2^n - 1$ with minimum distance $d = 2e+1 = 5$ and covering radius $\rho = e+1 = 3$.*

• We have seen that all AB functions are APN. The converse is false, in general. But if n is odd and if F is APN, then, as shown in [45, 42], there exists a nice necessary and sufficient condition, for F being AB: the weights of $C_F^\perp$ are all divisible by $2^{\frac{n-1}{2}}$ (see also [46], where the divisibilities for several types of such codes are calculated, where tables of exact divisibilities are computed and where proofs are given that a great deal of power functions are not AB). In other words:

Proposition 15 *Let F be an APN (n,n)-function, n odd. Then F is AB if and only if all the values $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ of the Walsh spectrum of F are divisible by $2^{\frac{n+1}{2}}$.*

Proof. The condition is clearly necessary. Conversely, assume that F is APN and that all the values $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ are divisible by $2^{\frac{n+1}{2}}$. Writing $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 = 2^{n+1}\lambda_{u,v}$, where all $\lambda_{u,v}$'s are integers, Relation (13) implies then

$$\sum_{v\in\mathbb{F}_2^{n*},u\in\mathbb{F}_2^n}(\lambda_{u,v}^2-\lambda_{u,v}) = 0, \tag{15}$$

and since all the integers $\lambda_{u,v}^2 - \lambda_{u,v}$ are non-negative ($\lambda_{u,v}$ being an integer), we deduce that $\lambda_{u,v}^2 = \lambda_{u,v}$ for every $v \in \mathbb{F}_2^{n*}, u \in \mathbb{F}_2^n$, *i.e.* $\lambda_{u,v} \in \{0,1\}$. □

Hence, if an APN function F is plateaued, or more generally if $F = F_1 \circ F_2^{-1}$ where F_2 is a permutation and where the linear combinations of the component functions of F_1 and F_2 are plateaued, then F is AB. Indeed, the sum $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x} = \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F_1(x)\oplus u\cdot F_2(x)}$ is then divisible by $2^{\frac{n+1}{2}}$. This allows to deduce easily the AB property of Gold and Kasami functions (see their definitions below) from their APN property, since the Gold functions are quadratic and the Kasami functions are equal, when n is odd, to $F_1 \circ F_2^{-1}$ where $F_1(x) = x^{2^{3i}+1}$ and $F_2(x) = x^{2^i+1}$ are quadratic[14].

[14] It is conjectured that the component functions of the Kasami functions are plateaued for every n even too. This is already proved in [82, Theorem 11] when n is not divisible by 6.

In the case n even: If F is APN, then there must exist $v \in \mathbb{F}_2^{n*}, u \in \mathbb{F}_2^n$ such that $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ is not divisible by $2^{(n+2)/2}$. Indeed, suppose that all the Walsh values of F have such divisibility. Then denoting again $\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}\right)^2 = 2^{n+1}\lambda_{u,v}$, we have Relation (15). All the values $\lambda_{u,v}^2 - \lambda_{u,v}$ are non-negative integers and (for each $v \neq 0$) at least one value is strictly positive, a contradiction. If all the Walsh values of F are divisible by $2^{n/2}$ (*e.g.* if F is plateaued), then we deduce that there must exist $v \in \mathbb{F}_2^{n*}, u \in \mathbb{F}_2^n$ such that $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x}$ is congruent with $2^{n/2}$ modulo $2^{n/2+1}$. Hence, if F is plateaued, there must exist $v \in \mathbb{F}_2^{n*}$ such that the Boolean function $v\cdot F$ is bent. *Note that this implies that F cannot be a permutation*, according to Proposition 2 and since a bent Boolean function is never balanced. More precisely, when F is plateaued and APN, the numbers $\lambda_{u,v}$ involved in Equation (15) can be divided into two categories: those such that the function $v\cdot F$ is bent (for each such v, we have $\lambda_{u,v} = 1/2$ for every u and therefore $\sum_{u\in\mathbb{F}_2^n}(\lambda_{u,v}^2 - \lambda_{u,v}) = -2^{n-2}$); and those such that $v\cdot F$ is not bent (then $\lambda_{u,v} \in \{0, 2^i\}$ for some $i \geq 1$ depending on v, and therefore $\lambda_{u,v}^2 = 2^i\lambda_{u,v}$ and we have, thanks to Parseval's relation applied to the Boolean function $v\cdot F$: $\sum_{u\in\mathbb{F}_2^n}(\lambda_{u,v}^2 - \lambda_{u,v}) = (2^i-1)\sum_{u\in\mathbb{F}_2^n}\lambda_{u,v} = (2^i - 1)\frac{2^{2n}}{2^{n+1}} = (2^i-1)2^{n-1} \geq 2^{n-1}$). Equation (15) implies then that the number B of those v such that $v\cdot F$ is bent satisfies $-B\,2^{n-2} + (2^n - 1 - B)\,2^{n-1} \leq 0$, which implies that *the number of bent functions among the functions $v\cdot F$ is at least $\frac{2}{3}(2^n-1)$*.

In the case of the Gold functions $F(x) = x^{2^i+1}$, $gcd(i,n) = 1$ (see Subsection 3.1.7), the number of bent functions among the functions $tr_n(vF(x))$ equals $\frac{2}{3}(2^n-1)$. Indeed, according to the results recalled in the section on bent functions of the previous chapter, the function $tr_n(vF(x))$ is bent if and only if v is not the third power of an element of $\mathbb{F}_{2^n}$.

Note that, given an APN plateaued function F, saying that the number of bent functions among the functions $tr_n(vF(x))$ equals $\frac{2}{3}(2^n-1)$ is equivalent to saying, according to the observations above, that there is no v such that $\lambda_{u,v} = \pm 2^i$ with $i > \frac{n}{2}+1$, that is, F has nonlinearity $2^{n-1} - 2^{n/2}$ and it is also equivalent to saying that F has the same extended Walsh spectrum as the Gold functions.

The fact that an APN function F has same extended Walsh spectrum as the Gold functions can be characterized by using a similar method as for proving Proposition 11: this situation happens if and only if, for every $v \in \mathbb{F}_2^{n*}$ and every $u \in \mathbb{F}_2^n$, we have $\widehat{1_{G_F}}(u,v) \in \{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$ (where

$\widehat{1_{G_F}}(u,v) = \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)\oplus u\cdot x})$, that is

$$\widehat{1_{G_F}}(u,v)\left(\widehat{1_{G_F}}^2(u,v) - 2^{n+2}\right)\left(\widehat{1_{G_F}}^2(u,v) - 2^n\right) = 0,$$

or equivalently $\widehat{1_{G_F}}^5(u,v) - 5\cdot 2^n\,\widehat{1_{G_F}}^3(u,v) + 2^{2n+2}\widehat{1_{G_F}}(u,v) = 0$. Applying the Fourier transform and dividing by 2^{2n}, this is equivalent to the fact that

$$\left|\left\{(x_1,\cdots,x_5)\in\mathbb{F}_2^{5n}/\left\{\begin{array}{l}\sum_{i=0}^5 x_i = a\\ \sum_{i=0}^5 F(x_i) = b\end{array}\right.\right\}\right| - 2^{3n} -$$

$$5\cdot 2^n\left(\left|\left\{(x_1,\cdots,x_3)\in\mathbb{F}_2^{3n}/\left\{\begin{array}{l}\sum_{i=0}^3 x_i = a\\ \sum_{i=0}^3 F(x_i) = b\end{array}\right.\right\}\right| - 2^n\right) +$$

$$2^{2n+2}\left(\left|\left\{x\in\mathbb{F}_2^n/\left\{\begin{array}{l}x = a\\ F(x) = b\end{array}\right.\right\}\right| - 2^{-n}\right) = 0$$

for every $a,b\in\mathbb{F}_2^n$. A necessary condition is (taking $b = F(a)$ and using that F is APN) that, for every $a,b\in\mathbb{F}_2^n$, we have

$$\left|\left\{(x_1,\cdots,x_5)\in\mathbb{F}_2^{5n}/\left\{\begin{array}{l}\sum_{i=0}^5 x_i = a\\ \sum_{i=0}^5 F(x_i) = b\end{array}\right.\right\}\right| =$$

$$2^{3n} + 5\cdot 2^n(3\cdot 2^n - 2 - 2^n) - 2^{2n+2}(1-2^{-n}) =$$

$$2^{3n} + 3\cdot 2^{2n+1} - 3\cdot 2^{n+1}.$$

There exist APN quadratic functions whose Walsh spectra are different from the Gold functions. K. Browning *et al.* [23] have exhibited such function in 6 variables: $F(x) = x^3 + \alpha^{11}x^5 + \alpha^{13}x^9 + x^{17} + \alpha^{11}x^{33} + x^{48}$, where α is a primitive element in the field. For this function, we get the following spectrum: 46 functions $tr_6(vF(x))$ are bent, 16 are plateaued with amplitude 16 and one is plateaued with amplitude 32. □

3.1.4 The particular case of power functions

We have seen that the notion of AB function being independent of the choice of the inner product, we can identify $\mathbb{F}_2^n$ with the field $\mathbb{F}_{2^n}$ and take $x\cdot y = tr_n(xy)$ for inner product (where tr_n is the trace function from this field to $\mathbb{F}_2$). This allows to consider those particular (n,n)-functions which have the form $F(x) = x^d$, called *power functions* (and sometimes, *monomial functions*).

When F is a power function, it is enough to check the APN property for

$a = 1$ only, since changing, for every $a \neq 0$, the variable x into ax in the equation $F(x) + F(x+a) = b$ gives $F(x) + F(x+1) = \frac{b}{F(a)}$. Note that this implies that if a power function from $\mathbb{F}_{2^n}$ to itself is APN then for every m dividing n, this power function is APN as a function from $\mathbb{F}_{2^m}$ to itself. Moreover, checking the AB property $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vF(x)+ux)} \in \{0, \pm 2^{\frac{n+1}{2}}\}$, for every $u, v \in \mathbb{F}_{2^n}$, $v \neq 0$, is enough for $u = 0$ and $u = 1$ (and every $v \neq 0$), since changing x into $\frac{x}{u}$ (if $u \neq 0$) in this sum gives $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(v'F(x)+x)}$, for some $v' \neq 0$. If F is a permutation, then checking the AB property is also enough for $v = 1$ and every u, since changing x into $\frac{x}{F^{-1}(v)}$in this sum gives $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n\left(F(x)+\frac{u}{F^{-1}(v)}x\right)}$.
Also, when F is an APN power function, we have additional information on its bijectivity. It was proved in [56] that, when n is even, no APN function exists in a class of permutations including power permutations, that we describe now. Let $k = \frac{2^n-1}{3}$ (which is an integer, since n is even) and let α be a primitive element of the field $\mathbb{F}_{2^n}$. Then $\beta = \alpha^k$ is a primitive element of $\mathbb{F}_4$. Hence, $\beta^2+\beta+1 = 0$. For every j, the element $(\beta+1)^j + \beta^j = \beta^{2j} + \beta^j$ equals 1 if j is coprime with 3 (since β^j is then also a primitive element of $\mathbb{F}_4$), and is null otherwise. Let $F(x) = \sum_{j=0}^{2^n-1} \delta_j x^j$, ($\delta_j \in \mathbb{F}_{2^n}$) be an (n,n)-function. According to the observations above, β and $\beta+1$ are the solutions of the equation $F(x)+F(x+1) = \sum_{gcd(j,3)=1} \delta_j$. Also, the equation $F(x) + F(x+1) = \sum_{j=1}^{2^n-1} \delta_j$ admits 0 and 1 for solutions. Thus:

Proposition 16 *Let n be even and let $F(x) = \sum_{j=0}^{2^n-1} \delta_j x^j$ be any APN (n,n)-function, then $\sum_{j=1}^{k} \delta_{3j} \neq 0$, $k = \frac{2^n-1}{3}$. If F is a power function, then it can not be a permutation.*

H. Dobbertin gives in [91] a result valid only for power functions but slightly more precise, and he completes it in the case that n is odd:

Proposition 17 *If a power function $F(x) = x^d$ over $\mathbb{F}_{2^n}$ is APN, then for every $x \in \mathbb{F}_{2^n}$, we have $x^d = 1$ if and only if $x^3 = 1$, that is, $F^{-1}(1) = \mathbb{F}_4 \cap \mathbb{F}_{2^n}^*$. If n is odd, then $gcd(d, 2^n-1)$ equals 1 and, if n is even, then $gcd(d, 2^n-1)$ equals 3. Consequently, APN power functions are permutations if n is odd, and are three-to-one if n is even.*

Proof. Let $x \neq 1$ be such that $x^d = 1$. There is a (unique) y in $\mathbb{F}_{2^n}$, $y \neq 0, 1$, such that $x = (y+1)/y$. The equality $x^d = 1$ implies then $(y+1)^d + y^d = 0 = (y^2+1)^d + (y^2)^d$. By the APN property and since $y^2 \neq y$, we conclude $y^2+y+1 = 0$. Thus, y, and therefore x, are in $\mathbb{F}_4$ and $x^3 = 1$. Conversely, if $x \neq 1$ is an element of $\mathbb{F}_{2^n}^*$ such that $x^3 = 1$, then 3 divides 2^n-1 and n must be even. Moreover, d must also be divisible by 3 (indeed, otherwise, the restriction of x^d to $\mathbb{F}_4$ would coincide with the function $x^{gcd(d,3)}=x$ and would be therefore linear, a contradiction). Hence, we have $x^d=1$. The rest is straightforward. □

A. Canteaut proves in [43] that for n even, if a power function $F(x)=x^d$ on $\mathbb{F}_{2^n}$ is not a permutation (*i.e.* if $gcd(d,2^n-1)>1$), then the nonlinearity of F is bounded above by $2^{n-1}-2^{n/2}$ (she also studies the case of equality). Indeed, denoting $gcd(d,2^n-1)$ by d_0, then for every $v\in\mathbb{F}_{2^n}$, the sum $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vx^d)}$ equals $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vx^{d_0})}$ which implies that $\sum_{v\in\mathbb{F}_{2^n}}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vx^d)}\right)^2$ equals $2^n\,|\{(x,y),\ x,y\in\mathbb{F}_{2^n},\ x^{d_0}=y^{d_0}\}|$. The number of elements in the image of $\mathbb{F}_{2^n}^*$ by the mapping $x\to x^{d_0}$ is $(2^n-1)/d_0$ and every element of this image has d_0 pre-images. Hence, $\sum_{v\in\mathbb{F}_{2^n}^*}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vx^d)}\right)^2$ equals $2^n[(2^n-1)d_0+1]-2^{2n}=2^n(2^n-1)(d_0-1)$ and $\max_{v\in\mathbb{F}_{2^n}^*}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vx^d)}\right)^2\geq 2^n(d_0-1)\geq 2^{n+1}$. The possible values of the sum $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vx^d)}$ are determined in [7] for APN power functions in an even number of variables.

If F is a power function, then the linear codes C_F and $C_F^\perp$ (viewed in Proposition 12) are *cyclic codes*, that is, are invariant under cyclic shifts of their coordinates (see [130] and the chapter "Boolean Functions for Cryptography and Error Correcting Codes"). Indeed, $(c_0,\dots,c_{2^n-2})$ belongs to C_F if and only if $c_0+c_1\alpha+\ldots+c_{2^n-2}\alpha^{2^n-2}=0$ and $c_0+c_1\alpha^d+\ldots+c_{2^n-2}\alpha^{(2^n-2)d}=0$; this implies (by multiplying these equations by α and α^d, respectively) $c_{2^n-2}+c_0\alpha+\ldots+c_{2^n-3}\alpha^{2^n-2}=0$ and $c_{2^n-2}+c_0\alpha^d+\ldots+c_{2^n-3}\alpha^{(2^n-2)d}=0$. Recall that, representing each codeword $(c_0,c_1,\cdots,c_{2^n-2})$ by the element $\sum_{i=0}^{2^n-2}c_iX^i$ of the algebra $\mathbb{F}_2[X]/(X^{2^n-1}+1)$, the code is then an ideal of this algebra and it equals the set of all those polynomials of degrees at most 2^n-2 which are multiples (as elements of the algebra and more strongly as polynomials) of a polynomial, called generator polynomial, dividing $X^{2^n-1}+1$, which is the unique element of minimal degree in the code. In other words, $\sum_{i=0}^{2^n-2}c_iX^i$ is a codeword if and only if the roots in $\mathbb{F}_{2^n}$ of the generator polynomial are also roots of $\sum_{i=0}^{2^n-2}c_iX^i$. The roots of the generator polynomial are of the form $\{\alpha^i,\ i\in I\}$ where $I\subseteq\mathbb{Z}/(2^n-1)\mathbb{Z}$ is a union of cyclotomic classes of 2 modulo 2^n-1. The set I is called the *defining set* of the code. In the case of C_F, the defining set I is precisely the union of the two cyclotomic classes containing 1 and d.

A very efficient bound on the minimum distance of cyclic codes, also recalled in the previous chapter, is the *BCH bound* [130]: if I contains a string $\{l+1,\dots,l+k\}$ of length k in $\mathbb{Z}/(2^n-1)\mathbb{Z}$, then the cyclic code has minimum distance greater than or equal to $k+1$. This bound shows for instance in an original way that the function $x^{2^{\frac{n-1}{2}}+1}$, n odd, is AB: by definition, the defining set I of C_F equals the union of the cyclotomic classes of 1 and $2^{\frac{n-1}{2}}+1$, that is

$$\{1,2,\cdots,2^{n-1}\}\cup$$
$$\{2^{\frac{n-1}{2}}+1, 2^{\frac{n+1}{2}}+2,\cdots,2^{n-1}+2^{\frac{n-1}{2}}, 2^{\frac{n+1}{2}}+1, 2^{\frac{n+3}{2}}+2,\cdots,2^{n-1}+2^{\frac{n-3}{2}}\}.$$

The defining set of $C_F^\perp$ equals then $\mathbb{Z}/(2^n-1)\mathbb{Z}\setminus\{-i;\ i\notin I\}$ (this property is valid for every cyclic code, see [130]). Since there is no element equal to $2^{n-1}+2^{\frac{n-1}{2}}+1,\cdots,2^n-1$ in I, the defining set of $C_F^\perp$ contains then a string of length $2^{n-1}-2^{\frac{n-1}{2}}-1$. Hence the nonzero codewords of this code have weights greater than or equal to $2^{n-1}-2^{\frac{n-1}{2}}$. This is not sufficient for concluding that the function is AB (since we need also to know that the complements of the extended codewords have weight at least $2^{n-1}-2^{\frac{n-1}{2}}$), but we can apply the previous reasoning to the cyclic code $C_F^\perp\cup((1,\cdots,1)+C_F^\perp)$: the defining set of the dual of this code being equal to that of C_F, plus 0, the defining set of the code itself equals that of $C_F^\perp$ less 0, which gives a string of length $2^{n-1}-2^{\frac{n-1}{2}}-2$ instead of $2^{n-1}-2^{\frac{n-1}{2}}-1$. Hence the complements of the codewords of $C_F^\perp$ have weights at least $2^{n-1}-2^{\frac{n-1}{2}}-1$, and since for these codewords, the corresponding Boolean function takes value 1 at the zero vector (which is not taken into account in the corresponding codeword), this allows now to deduce that all functions $tr_n(vx^{2^{\frac{n-1}{2}}+1}+ux)\oplus\epsilon$, $v\neq 0$, $\epsilon\in\mathbb{F}_2$, have weights between $2^{n-1}-2^{\frac{n-1}{2}}$ and $2^{n-1}+2^{\frac{n-1}{2}}$, that is, F is AB.
The powerful *McEliece Theorem* (see *e.g.* [130]) gives the exact divisibility of the codewords of cyclic codes. Translated in terms of vectorial functions, it says that if d is relatively prime to 2^n-1, the exponent e_d of the greatest power of 2 dividing all the Walsh coefficients of the power function x^d is given by $e_d=\min\{w_2(t_0)+w_2(t_1),\ 1\le t_0,\, t_1<2^n-1;\ t_0+t_1d\equiv 0\ [\bmod\ 2^n-1]\}$. It can be used in relationship with Proposition 15. This led to the proof, by Canteaut, Charpin and Dobbertin, of a several decade old conjecture due to Welch (see below).

Note finally that, if F is a power function, then the Boolean function γ_F seen in Proposition 10 is within the framework of Dobbertin's triple construction [83].

3.1.5 Notions of equivalence respecting the APN and AB properties

The right and left compositions of an APN (resp. AB) function by an affine permutation are APN (resp. AB). Two functions are called *affine equivalent* if one is equal to the other, composed by such affine permutations.
Adding an affine function to an APN (resp. AB) function respects its APN (resp. AB) property. Two functions are called *extended affine equivalent* (EA-equivalent) if one is affine equivalent to the other, added with an affine function.
The inverse of an APN (resp. AB) permutation is APN (resp. AB) but is in general not EA-equivalent to it. There exists a notion of equivalence between (n,n)-functions which respects APNness and ABness and for which any permutation is equivalent to its inverse. As we shall see, this equivalence relation is still more general than EA-equivalence between functions, up to replacing the functions by their inverses when they are permutations.

Definition 11 *Two (n,n)-functions F and G are called* CCZ-equivalent[15] *if their graphs $C_F = \{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \,|\, y = F(x)\}$ and $C_G = \{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \,|\, y = G(x)\}$ are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $y = F(x) \Leftrightarrow L_2(x,y) = G(L_1(x,y))$.*

As observed in [23], given two (n,n)-functions F and G such that $F(0) = G(0) = 0$, there exists a linear automorphism[16] which maps G_F to G_G if and only if the codes C_F and C_G (see the definition of these codes in Proposition 12) are equivalent (that is, are equal up to some permutation of the coordinates of their codewords). Indeed, the graph G_F of F equals the (unordered) set of columns in the parity-check matrix of the code C_F, plus an additional point equal to the all-zero vector. Hence, the existence of a linear automorphism which maps G_F onto G_G is equivalent to the fact that the parity-check matrices[17] of the codes C_F and C_G are equal up to multiplication (on the left) by an invertible matrix and to permutation of the columns. Since two codes with given parity-check matrices are equal if and only if these matrices are equal up to multiplication on the left by an invertible matrix, this completes the proof. It is nicely deduced in [23] that

[15] This notion has been introduced in [56] and later named CCZ-equivalence in [26, 27]; it could be also called graph-equivalence.

[16] Note that this is a sub-case of CCZ-equivalence - in fact, a strict sub-case as shown in [23].

[17] This is true also for the generator matrices of the codes.

two functions F and G taking any values at 0 are CCZ-equivalent if and only if the codes $\widetilde{C_F}$ and $\widetilde{C_G}$ (see the definition of these codes in the remark - alinea 2 - following Proposition 12) are equivalent.

The notion of CCZ-equivalence can be similarly defined for functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$.

Given a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, the image of the graph of F by L is the graph of a function if and only if the function $F_1(x) = L_1(x, F(x))$ is a permutation of $\mathbb{F}_2^n$. Indeed, if F_1 is a permutation then $L(G_F)$ equals the graph of the function $G = F_2 \circ F_1^{-1}$; and conversely, denoting $F_2(x) = L_2(x, F(x))$, the image of the graph of F by L equals $\{(F_1(x), F_2(x)); x \in \mathbb{F}_2^n\}$ and since L is a permutation, if $F_1(x) = F_1(x')$ for some $x \neq x'$ then $F_2(x) \neq F_2(x')$, and $L(G_F)$ is not the graph of a function.

Proposition 18 *If two (n, n)-functions F and G are CCZ-equivalent then F is APN (resp. AB) if and only if G is APN (resp. AB). Moreover, denoting by $L = (L_1, L_2)$ an affine automorphism between the graphs of F and G, the function γ_F (see Proposition 10) equals $\gamma_G \circ \mathcal{L}$, where $\mathcal{L}$ is the linear automorphism such that $L = \mathcal{L} + cst$.*

Proof. We have seen that $G = F_2 \circ F_1^{-1}$, where $F_1(x) = L_1(x, F(x))$ and $F_2(x) = L_2(x, F(x))$. The value $\gamma_G(a, b)$ equals 1 if and only if $a \neq 0$ and there exists (x, y) in $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $F_1(x) + F_1(y) = a$ and $F_2(x) + F_2(y) = b$, that is, $\mathcal{L}(x, F(x)) + \mathcal{L}(y, F(y)) = \mathcal{L}(x + y, F(x) + F(y)) = (a, b)$. Thus, γ_G is equal to $\gamma_F \circ \mathcal{L}^{-1}$. The function γ_G is therefore bent (resp. has weight $2^{2n-1} - 2^{n-1}$) if and only if γ_F is bent (resp. has weight $2^{2n-1} - 2^{n-1}$). Proposition 10 completes the proof. □

All the transformations respecting the APN (resp. AB) property that we have seen previously to Proposition 18 are particular cases of this general one:

- if $L_1(x, y)$ only depends on x, then writing $L_1(x, y) = L_1(x)$ and $L_2(x, y) = L'(x) + L''(y)$, the function $F_1(x) = L_1(x)$ is a permutation (since L being onto $\mathbb{F}_2^n \times \mathbb{F}_2^m$, L_1 must be onto $\mathbb{F}_2^n$) and we have $F_2 \circ F_1^{-1}(x) = L' \circ L_1^{-1}(x) + L'' \circ F \circ L_1^{-1}(x)$; this corresponds to EA-equivalence;
- if $(L_1, L_2)(x, y) = (y, x)$, then $F_2(x) = x$ and $F_1(x) = F(x)$; if F is a permutation then F_1 is a permutation and $F_2 \circ F_1^{-1}$ is equal to F^{-1}.

It has been proved in [26, 27] that CCZ-equivalence is strictly more general than EA-equivalence between the functions or their inverses (when they

exist), by exhibiting (see below) APN functions which are CCZ-equivalent to the APN function $F(x) = x^3$ on $\mathbb{F}_{2^n}$, but which are provably EA-inequivalent to it and (for n odd) to its inverse.
Note however that if we reduce ourselves to bent functions, then CCZ-equivalence and EA-equivalence coincide: let F be a bent (n,m)-function (n even, $m \leq n/2$) and let (without loss of generality) L_1 and L_2 be two linear functions from $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to (respectively) $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, such that (L_1, L_2) and $L_1(x, F(x))$ are permutations. For every vector v in $\mathbb{F}_2^n$, the function $v \cdot L_1(x, F(x))$ is necessarily unbent since, if $v = 0$ then it is null and if $v \neq 0$ then it is balanced, according to Proposition 2. Let us denote $L_1(x,y) = L'(x) + L''(y)$. We have then $F_1(x) = L'(x) + L'' \circ F(x)$. The adjoint operator L''' of L'' (satisfying by definition $v \cdot L''(y) = L'''(v) \cdot y$, that is, the linear function having for matrix the transpose of the matrix of L'') is then the null function, since if $L'''(v) \neq 0$ then $v \cdot F_1(x) = v \cdot L'(x) \oplus L'''(v) \cdot F(x)$ is bent. This means that L'' is null and L_1 depends then only on x, which corresponds to EA-equivalence.

Note that if (L_1, L_2) and (L_1, L_2') are linear permutations of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ and $F_1 = L_1(x, F(x))$ is a permutation of $\mathbb{F}_2^n$, then as shown in [24], the functions F' and F'' obtained by CCZ-equivalence from F by using (L_1, L_2) and (L_1, L_2') are EA-equivalent; so finding new EA-inequivalent functions by using CCZ-equivalence needs to find new permutations F_1, which is the difficult task.

Proving the CCZ-inequivalence between two functions is mathematically (and also computationally) difficult, unless some CCZ-invariant parameters can be proved different for the two functions. Examples of direct proofs of CCZ-inequivalence using only the definition can be found in [29, 30].
Examples of CCZ-invariant parameters are the following (see [23] and [94] where they are introduced and used):

- The extended Walsh spectrum.
- The equivalence class of the code $\widetilde{C_F}$ (under the relation of equivalence of codes), according to the result of [23] recalled after Definition 11, and all the invariants related to this code (the weight enumerator of $\widetilde{C_F}$, the weight enumerator of its dual - but it corresponds to the extended Walsh spectrum of the function - the automorphism group etc..., which coincide with some of the invariants below).
- The Γ-rank: let $\mathcal{G} = \mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$ be the so-called group algebra of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ over $\mathbb{F}_2$, consisting of the formal sums $\sum_{g \in \mathbb{F}_2^n \times \mathbb{F}_2^n} a_g \, g$ where

$a_g \in \mathbb{F}_2$. If S is a subset of $\mathbb{F}_2^n \times \mathbb{F}_2^n$, then it can be identified with the element $\sum_{s \in S} s$ of $\mathcal{G}$. The dimension of the ideal of $\mathcal{G}$ generated by the graph $G_F = \{(x, F(x));\ x \in \mathbb{F}_2^n\}$ of F is called the *Γ-rank* of F. The Γ-rank equals (see [94]) the rank of the matrix M_{G_F} whose term indexed by $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ and by $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ equals 1 if $(x, y) \in (a, b) + G_F$ and equals 0 otherwise.

- The Δ-rank, that is, the dimension of the ideal of $\mathcal{G}$ generated by the set $D_F = \{(a, F(x) + F(x + a));\ a,\ x \in \mathbb{F}_2^n;\ a \neq 0\}$ (recall that, according to Proposition 10, this set has size $2^{2n-1} - 2^{n-1}$ and is a difference set when F is AB). The Δ-rank equals the rank of the matrix M_{D_F} whose term indexed by (x, y) and by (a, b) equals 1 if $(x, y) \in (a, b) + D_F$ and equals 0 otherwise.

- The order of the automorphism group of the design $dev(G_F)$, whose points are the elements of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ and whose blocks are the sets $(a, b) + G_F$ (and whose incidence matrix is M_{G_F}), that is, of all those permutations on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ which map every such block to a block.

- The order of the automorphism group of the design $dev(D_F)$, whose points are the elements of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ and whose blocks are the sets $(a, b) + D_F$ (and whose incidence matrix is M_{D_F}).

- The order of the automorphism group $\mathcal{M}(G_F)$ of the so-called multipliers of G_F, that is, the permutations π of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $\pi(G_F)$ is a translate $(a, b) + G_F$ of G_F. This order is easier to compute and it allows in some cases to prove CCZ-inequivalence easily. As observed in [23], $\mathcal{M}(G_F)$ is the automorphism group of the code $\widetilde{C_F}$.

- The order of the automorphism group $\mathcal{M}(D_F)$.

CCZ-equivalence does not preserve crookedness nor the algebraic degree.

3.1.6 The known AB functions

Power functions: Until recently, the only known examples of AB functions were (up to EA-equivalence) the power functions $x \mapsto x^d$ on the field $\mathbb{F}_{2^n}$ (n odd) corresponding to the following values of d, and the inverses of these power functions:

• $d = 2^i + 1$ with $\gcd(i, n) = 1$ and $1 \leq i \leq \frac{n-1}{2}$ (proved by Gold, see [97, 137]). The condition $1 \leq i \leq \frac{n-1}{2}$ (here and below) is not necessary but we mention it because the other values of i give EA-equivalent functions. These power functions are called *Gold functions*.

- $d = 2^{2i} - 2^i + 1$ with $\gcd(i, n) = 1$ and $2 \leq i \leq \frac{n-1}{2}$ (the AB property of this function is equivalent to a result by Kasami [115], historically due to Welch, but never published by him; see another proof in [86]). These power functions are called *Kasami functions* (some authors call them *Kasami-Welch functions*).
- $d = 2^{(n-1)/2} + 3$ (conjectured by Welch and proved by Canteaut, Charpin and Dobbertin, see [87, 45, 46]). These power functions are called *Welch functions*.
- $d = 2^{(n-1)/2} + 2^{(n-1)/4} - 1$, where $n \equiv 1 \pmod 4$ (conjectured by Niho, proved by Hollman and Xiang, after the work by Dobbertin, see [88, 106]).
- $d = 2^{(n-1)/2} + 2^{(3n-1)/4} - 1$, where $n \equiv 3 \pmod 4$ (idem). The power functions in these two last cases are called *Niho functions*.

The almost bentness of these functions can be deduced from their almost perfect nonlinearity (see below) by using Proposition 15 (and McEliece's Theorem in the cases of the Welch and Niho functions; the proofs are then not easy). The direct proof that the Gold function is AB is easy by using the properties of quadratic functions recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", in the subsection devoted to quadratic functions. The value at a of the Walsh transform of the Gold Boolean function $tr_n(x^{2^i+1})$ equals $\pm 2^{\frac{n+1}{2}}$ if $tr_n(a) = 1$ and is null otherwise, since $tr_n(x^{2^i}y + xy^{2^i}) = tr_n((x^{2^i} + x^{2^{n-i}})\, y)$ is null for every y if and only if $x^{2^{2i}} + x = 0$, that is, if and only if $x \in \mathbb{F}_2$ (since $gcd(2^{2i} - 1, 2^n - 1) = 1$), and since $tr_n(x^{2^i+1} + ax)$ is constant on $\mathbb{F}_2$ if and only if $tr_n(a) = 1$. This gives easily the magnitude (but not the sign, which is studied in [123]) of the Walsh transform of the vectorial Gold function, this function being a permutation (see Subsection 3.1.4).
The inverse of x^{2^i+1} is x^d, where

$$d = \sum_{k=0}^{\frac{n-1}{2}} 2^{2ik},$$

and x^d has therefore the algebraic degree $\frac{n+1}{2}$ [137].
It has been proved in [81, Theorem 7] and [82, Theorem 15] that, if $3i$ is congruent with 1 mod n, then the Walsh support of the Kasami Boolean function $tr_n(x^{2^{2i}-2^i+1})$ equals the support of the Gold Boolean function $tr_n(x^{2^i+1})$ (*i.e.* the set $\{x \in \mathbb{F}_{2^n} \,|\, tr_n(x^{2^i+1}) = 1\}$) if n is odd and equals

the set $\{x \in \mathbb{F}_{2^n} \,|\, tr_{n/2}(x^{2^i+1}) = 0\}$ if n is even, where $tr_{n/2}$ is the trace function from $\mathbb{F}_{2^n}$ to the field $\mathbb{F}_{2^2}$: $tr_{n/2}(x) = x + x^4 + x^{4^2} + \ldots + x^{4^{n/2-1}}$. When n is odd, this gives the magnitude (but not the sign) of the Walsh transform of the vectorial Kasami function, this function being a permutation. Note that this gives also an information on the autocorrelation of the Kasami Boolean function: according to the Wiener-Khintchine theorem (see the previous chapter), the Fourier transform of the function $a \rightarrow \mathcal{F}(D_af) = \sum_{x\in\mathbb{F}_2^n}(-1)^{D_af(x)}$, where f is the Kasami Boolean function, equals the square of the Walsh transform of f. According to Dillon's and Dobbertin's result recalled above, and since we know that the Kasami function is almost bent when n is odd, the value at b of the square of the Walsh transform of f equals then 2^{n+1} if $tr_n(x^{2^i+1}) = 1$ and equals zero otherwise. Hence, by applying the inverse Fourier transform (that is, by applying the Fourier transform again and dividing by 2^n), $\mathcal{F}(D_af)$ equals twice the Fourier transform of the function $tr_n(x^{2^i+1})$. We deduce that, except at the zero vector, $\mathcal{F}(D_af)$ equals the opposite of the Walsh transform of the function $tr_n(x^{2^i+1})$.

It is proved in [30] that Gold functions are pairwise CCZ-inequivalent and that they are in general CCZ-inequivalent to Kasami and Welch functions.

We have seen that the Walsh value distribution of AB functions is known. A related result of [123] is generalized in [98]: for every AB power function x^d over $\mathbb{F}_{2^n}$ whose restriction to any subfield of $\mathbb{F}_{2^n}$ is also AB, the value $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(x^d+x)}$ equals $2^{\frac{n+1}{2}}$ if $n \equiv \pm1$ [mod 8] and $-2^{\frac{n+1}{2}}$ if $n \equiv \pm3$ [mod 8].

Remark. There is a close relationship between AB power functions and *sequences* used for radars and for spread-spectrum communications. A binary sequence which can be generated by an LFSR, or equivalently which satisfies a linear recurrence relation $s_i = a_1s_{i-1} \oplus \ldots \oplus a_ns_{i-n}$, is called an *m-sequence* or a *maximum-length sequence* if its period equals $2^n - 1$, which is the maximal possible value. Such a sequence has the form $tr_n(\lambda\alpha^i)$, where $\lambda \in \mathbb{F}_{2^n}$ and α is some primitive element of $\mathbb{F}_{2^n}$, and where tr_n is the trace function on $\mathbb{F}_{2^n}$. Consequently, its auto-correlation values $\sum_{i=0}^{2^n-2}(-1)^{s_i\oplus s_{i+t}}$ $(1 \leq t \leq 2^n-2)$ are equal to -1, that is, are optimum. Such a sequence can be used for radars and for code division multiple access (CDMA) in telecommunications, since it allows sending a signal which can be easily distinguished from any time-shifted version of itself. Finding an AB power function x^d on the field $\mathbb{F}_{2^n}$ allows to have a d-decimation[18] $s'_i = tr_n(\lambda\alpha^{di})$ of the sequence, whose cross-correlation values $\sum_{i=0}^{2^n-2}(-1)^{s_i \oplus s'_{i+t}}$ $(0 \leq t \leq 2^n - 2)$ with the sequence s_i have minimum overall magnitude[19] [101]. The cross-correlation is then called a *preferred cross-correlation* function, see [36]. The conjectures that the power functions above were AB have been stated (before being proved later) in the framework of sequences for this reason.

It has been conjectured by Hans Dobbertin that the list of power AB functions above is complete. See [126] about this conjecture.

Non-power functions: It was first conjectured that all AB functions are equivalent to power functions and to permutations. These two conjectures were later disproved, in a first step by exhibiting AB functions which are EA-inequivalent to power functions and to permutations, but which are by construction CCZ-equivalent to the Gold function $x \to x^3$, and in a second step by finding AB functions which are CCZ-inequivalent to power functions[20] (at least for some values of n):

Functions CCZ-equivalent to power functions:

Two examples of linear permutations over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ transforming the graph of the Gold function $x \to x^3$ into the graph of a function have been found in [26], giving new classes of AB functions:

• The function $F(x) = x^{2^i+1} + (x^{2^i} + x)\, tr_n(x^{2^i+1} + x)$, where $n > 3$ is odd and $gcd(n, i) = 1$, is AB. It is provably EA-inequivalent to any power function and it is EA-inequivalent to any permutation (at least for $n = 5$), which disproves a conjecture stated in [26].

• For n odd and divisible by m, $n \neq m$ and $\gcd(n, i) = 1$, the following function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$:

$$\begin{aligned}
&x^{2^i+1} + tr_{n/m}(x^{2^i+1}) + x^{2^i} tr_{n/m}(x) + x\; tr_{n/m}(x)^{2^i} + \\
&[tr_{n/m}(x)^{2^i+1} + tr_{n/m}(x^{2^i+1}) + tr_{n/m}(x)]^{\frac{1}{2^i+1}}(x^{2^i} + tr_{n/m}(x)^{2^i} + 1) + \\
&[tr_{n/m}(x)^{2^i+1} + tr_{n/m}(x^{2^i+1}) + tr_{n/m}(x)]^{\frac{2^i}{2^i+1}}(x + tr_{n/m}(x))
\end{aligned}$$

where $tr_{n/m}$ denotes the trace function $tr_{n/m}(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}$ from $\mathbb{F}_{2^n}$

[18] Another m-sequence if d is co-prime with $2^n - 1$.

[19] This allows, in code division multiple access, to give different signals to different users.

[20] The question of knowing whether all AB functions are CCZ-equivalent to permutations remains open, as far as we know.

to $\mathbb{F}_{2^m}$, is an AB function of algebraic degree $m+2$ which is provably EA-inequivalent to any power function; the question of knowing whether it is EA-inequivalent to any permutation is open.

Open problem: Find classes of AB functions by using CCZ-equivalence with Kasami (resp. Welch, Niho) functions.

• Though the AB functions constructed in [26] cannot be obtained from power functions by applying only EA-equivalence and inverse transformation, L. Budaghyan shows in [25] that AB functions EA-inequivalent to power functions can be constructed by only applying EA-equivalence and inverse transformation to power AB functions.

Functions CCZ-inequivalent to power functions:

The problem of knowing whether there exist AB functions which are CCZ-inequivalent to power functions remained open after the introduction of the two functions above. Also, it was conjectured that any quadratic APN function is EA-equivalent to Gold functions and this problem remained open. A paper by Edel, Kyureghyan and Pott [93] introduced two quadratic APN functions from $\mathbb{F}_{2^{10}}$ (resp. $\mathbb{F}_{2^{12}}$) to itself. The first one was proved to be CCZ-inequivalent to any power function.
These two (quadratic) functions were isolated and this left open the question of knowing whether a whole infinite class of APN/AB functions being not CCZ-equivalent to power functions could be exhibited.
• The new following class of AB functions was found in [28, 29]:

Proposition 19 *Let s and k be positive integers with $\gcd(s, 3k) = 1$ and $t \in \{1, 2\}$, $i = 3 - t$. Furthermore let $d = 2^{ik} + 2^{tk+s} - (2^s + 1)$,*

$$g_1 = \gcd(2^{3k} - 1, d/(2^k - 1)),$$

$$g_2 = \gcd(2^k - 1, d/(2^k - 1)).$$

If $g_1 \neq g_2$ then the function

$$\begin{array}{rcl} F : \mathbb{F}_{2^{3k}} & \rightarrow & \mathbb{F}_{2^{3k}} \\ x & \mapsto & \alpha^{2^k-1} x^{2^{ik}+2^{tk+s}} + x^{2^s+1} \end{array}$$

where α is primitive in $\mathbb{F}_{2^{3k}}$ is AB when k is odd and APN when k is even.

It could be proved in [28, 29] that some of these functions are EA-inequivalent to power functions and CCZ-inequivalent to some AB power functions, and this was sufficient to deduce that they are CCZ-inequivalent to all power functions for some values of n:

Proposition 20 *Let s and $k \geq 4$ be positive integers such that $s \leq 3k-1$, $\gcd(k,3) = \gcd(s,3k) = 1$, and $i = sk$ [mod 3], $t = 2i$ [mod 3], $n = 3k$. If $a \in \mathbb{F}_{2^n}$ has the order $2^{2k}+2^k+1$ then the function $F(x) = x^{2^s+1} + ax^{2^{ik}+2^{tk+s}}$ is an AB permutation on $\mathbb{F}_{2^n}$ when n is odd and is APN when n is even. It is EA-inequivalent to power functions and CCZ-inequivalent to Gold and Kasami mappings.*

- It has been shown in [32] that:

Proposition 21 *For every odd positive integer, the function $x^3 + tr_n(x^9)$ is AB on $\mathbb{F}_{2^n}$ (and that it is APN for n even).*

This function is the only example, with the function x^3, of a function which is AB for any odd n (if we consider it as the same function for every n which is not quite true since the trace function depends on n). It is CCZ-inequivalent to any Gold function on $\mathbb{F}_{2^n}$ if $n \geq 7$.

Open problem: Find infinite classes of AB functions CCZ-inequivalent to power functions and to quadratic functions.

3.1.7 The known APN functions

We list now the known APN functions (in addition to the AB functions listed above).

Power functions: The so-called *multiplicative inverse permutation* (or simply *inverse function*) $x \mapsto F(x) = x^{2^n-2}$ (which equals $\frac{1}{x}$ if $x \neq 0$, and 0 otherwise) is APN if n is odd [8, 137]. Indeed, the equation $x^{2^n-2} + (x+1)^{2^n-2} = b$ ($b \neq 0$, since the inverse function is a permutation) admits 0 and 1 for solutions if and only if $b = 1$; and it (also) admits (two) solutions different from 0 and 1 if and only if there exists $x \neq 0, 1$ such that $\frac{1}{x} + \frac{1}{x+1} = b$, that is, $x^2 + x = \frac{1}{b}$. It is well-known that such existence is equivalent to the fact that $tr_n\left(\frac{1}{b}\right) = 0$. Hence, F is APN if and only if $tr_n(1) = 1$, that is, if n is odd.
Consequently, the functions $x \mapsto x^{2^n-2^i-1}$, which are linearly equivalent to F (through the linear isomorphism $x \mapsto x^{2^i}$) are also APN, if n is odd.

If n is even, then the equation $x^{2^n-2}+(x+1)^{2^n-2}=b$ admits at most 2 solutions if $b\neq 1$ and admits 4 solutions (the elements of $\mathbb{F}_4$) if $b=1$, which means that F opposes a good (but not optimal) resistance against differential cryptanalysis. Its nonlinearity equals $2^{n-1}-2^{n/2}$ when n is even and it equals the highest even number bounded above by this number, when n is odd (see [64]; Lachaud and Wolfmann proved in [122] that the set of values of its Walsh spectrum equals the set of all integers $s\equiv 0$ [mod 4] in the range $[-2^{n/2+1}+1; 2^{n/2+1}+1]$; see more in [104]). Knowing whether there exist (n,n)-functions with nonlinearity strictly greater than this value when n is even is an open question (even for power functions). These are some of the reasons why the function $x\mapsto x^{2^n-2}$ has been chosen for the S-boxes of the AES.

Until recently, the only known examples of APN functions were (up to affine equivalence and to the addition of an affine function) power functions $x\mapsto x^d$. We list below the known values of d for which we obtain APN functions, without repeating the cases where the functions are AB:

- $d=2^n-2$, n odd (inverse function);
- $d=2^i+1$ with $\gcd(i,n)=1$, n even and $1\le i\le\frac{n-2}{2}$ (*Gold functions*, see [97, 137]);
- $d=2^{2i}-2^i+1$ with $\gcd(i,n)=1$, n even and $2\le i\le\frac{n-2}{2}$ (*Kasami functions*, see [111], see also [86]);
- $d=2^{\frac{4n}{5}}+2^{\frac{3n}{5}}+2^{\frac{2n}{5}}+2^{\frac{n}{5}}-1$, with n divisible by 5 (*Dobbertin functions*, see [89]). It has been shown by Canteaut, Charpin and Dobbertin [46] that this function can not be AB: they showed that $C_F^\perp$ contains words whose weights are not divisible by $2^{\frac{n-1}{2}}$.

The proof that the Gold functions are APN (whatever is the parity of n) is easy: the equality $F(x)+F(x+1)=F(y)+F(y+1)$ is equivalent to $(x+y)^{2^i}=(x+y)$, and thus implies that $x+y=0$ or $x+y=1$, since i and n are co-prime. Hence, any equation $F(x)+F(x+1)=b$ admits at most two solutions.

The proofs that the Kasami and Dobbertin functions are APN are difficult. They come down to showing that some mappings are permutations. H. Dobbertin gives in [90] a nice general method for this.

The Gold and Kasami functions, for n even, have the best known nonlinearity when n is even too [97, 115], but not the Dobbertin functions. See [46] for a list of all known *permutations* with best known nonlinearity. See also [84].

Inverse and Dobbertin functions are CCZ-inequivalent to all other known APN functions because of their peculiar Walsh spectra.
It is proven in [21] that there exists no APN function CCZ-inequivalent to power mappings on $\mathbb{F}_{2^n}$ for $n \leq 5$.
The exponents d such that the function x^d is APN on infinitely many fields $\mathbb{F}_{2^n}$ have been called *exceptional* by J. Dillon (see *e.g.* [23]). We have seen above that a power function x^d is APN if and only if the function $x^d + (x+1)^d + 1$ (we write ‘ +1” so that 0 is a root, which simplifies presentation) is 2-to-1. For every (n,n)-function F over $\mathbb{F}_{2^n}$, there clearly always exists a polynomial P such that $F(x)+F(x+1)+F(1) = P(x+x^2)$. J. Dillon observed that, in the cases of the Gold and Kasami functions, the polynomial P is an exceptional polynomial (*i.e.* is a permutation over infinitely many fields $\mathbb{F}_{2^n}$); from there comes the term. In the case of the Gold function x^{2^i+1}, we have $P(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{i-1}}$ which is a linear function over the algebraic closure of $\mathbb{F}_2$ having kernel $\{x \in \mathbb{F}_{2^i} \,/\, tr_i(x) = 0\}$ and is therefore a permutation over $\mathbb{F}_{2^n}$ for every n co-prime with i. In the case of the Kasami function, $P(x) = \frac{(tr_i(x))^{2^i+1}}{x^{2^i}}$ is the Müller-Cohen-Matthews polynomial [71]. It is conjectured that the Gold and Kasami exponents are the only exceptional exponents.

Non-power functions: As for AB functions, it had been conjectured that all APN functions were EA-equivalent to power functions and this conjecture was proven false:

Functions CCZ-equivalent to power functions:

Using also the stability properties recalled in Subsection 3.1.5, two more infinite classes of APN functions have been introduced in [26] and disprove the conjecture above:
- The function $F(x) = x^{2^i+1} + (x^{2^i} + x + 1)\, tr_n(x^{2^i+1})$, where $n \geq 4$ is even and $gcd(n,i) = 1$ is APN and is EA-inequivalent to any power function.
- For n even and divisible by 3, the function $F(x)$ equal to

$$[x + tr_{n/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr_n(x)\, tr_{n/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1},$$

where $gcd(n,i) = 1$, is APN and is EA-inequivalent to any known APN function.

Open problem: Find classes of APN functions by using CCZ-equivalence with Kasami (resp. Welch, Niho, Dobbertin, inverse) functions.

Functions CCZ-inequivalent to power functions:

• As recalled above, the paper [93] introduced two quadratic APN functions from $\mathbb{F}_{2^{10}}$ (resp. $\mathbb{F}_{2^{12}}$) to itself. The first one: $F(x) = x^3 + ux^{36}$, where $u \in \mathbb{F}_4 \setminus \mathbb{F}_2$, was proved to be CCZ-inequivalent to any power function by computing its Δ-rank.
The functions viewed in Proposition 19 are APN when n is even and generalize the second function: $F(x) = x^3 + \alpha^{15}x^{528}$, where α is a primitive element of $\mathbb{F}_{2^{12}}$; some of them can be proven CCZ inequivalent to Gold and Kasami mappings, as seen in Proposition 20. A similar class but with n divisible by 4 was later given in [31]. As observed by J. Bierbrauer, a common framework exists for the class of Proposition 20 and this new class:

Theorem 2 *Let:*
- $n = tk$ be a positive integer, with $t \in \{3, 4\}$, and s be such that t, s, k are pairwise coprime and such that t is a divisor of $k + s$,
- α be a primitive element of $\mathbb{F}_{2^n}$ and $w = \alpha^e$, where e is a multiple of $2^k - 1$, coprime with $2^t - 1$,
then the function

$$F(x) = x^{2^s+1} + wx^{2^{k+s}+2^{k(t-1)}}$$

is APN.

For $n \geq 12$, these functions are EA-inequivalent to power functions and CCZ-inequivalent to Gold and Kasami mappings [29].
In particular, for $n = 12$, 20, 24, 28 they are CCZ-inequivalent to all power functions.
• Proposition 20 has been generalized[21] in [16, 17] by C. Bracken, E. Byrne, N. Markin and G. McGuire:

$$F(x) = u^{2^k}x^{2^{2k}+2^{k+s}} + ux^{2^s+1} + vx^{2^{2k}+1} + wu^{2^k+1}x^{2^{k+s}+2^s}$$

is APN on $\mathbb{F}_{2^{3k}}$, when $3 \,|\, k + s$, $(s, 3k) = (3, k) = 1$ and u is primitive in $\mathbb{F}_{2^{3k}}$, $v \neq w^{-1} \in \mathbb{F}_{2^k}$.
The same authors in the same paper obtained another class of APN functions:

$$F(x) = bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^k+1} + \sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}$$

[21] Note that Proposition 19 covers a larger class of APN functions than Proposition 20.

where k, s are odd and coprime, $b \in \mathbb{F}_{2^{2k}}$ is not a cube, $c \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$, $r_i \in \mathbb{F}_{2^k}$ is APN on $\mathbb{F}_{2^{2k}}$.
The extended Walsh spectrum of these functions is the same as for Gold function, see [14]. But it is proved in [18] that at least some of these functions are inequivalent to Gold functions.

• As already mentioned, the construction of AB functions of Proposition 21 gives APN functions for n even: *for any positive integer n, the function $x^3 + tr_n(x^9)$ is APN on $\mathbb{F}_{2^n}$.*
This function is CCZ-inequivalent to any Gold function on $\mathbb{F}_{2^n}$ if $n \geq 7$.
The extended Walsh spectrum of this function is the same as for the Gold functions as shown in [13].

• An idea of J. Dillon [79] was that (n, n)-functions (over $\mathbb{F}_{2^n}$) of the form:

$$F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q},$$

where $q = 2^{n/2}$, n even, have good chances to be differentially 4-uniform. This idea was exploited and pushed further in [33], which gave new APN functions:

Proposition 22 *Let n be even and i be co-prime with $n/2$. Set $q = 2^{n/2}$ and let $c, b \in \mathbb{F}_{2^n}$ be such that $c^{q+1} = 1$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $cb^q + b \neq 0$. Then the function*

$$F(x) = x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$$

is APN on $\mathbb{F}_{2^n}$.
Such vectors b, c do exist if and only if $\gcd(2^i + 1, q + 1) \neq 1$. *For $n/2$ odd, this is equivalent to saying that i is odd.*

The extended Walsh spectrum of these functions is the same as that of the Gold functions [163].

• Another class was obtained in this same paper [33] with the same idea:

Proposition 23 *Let n be even and i be co-prime with $n/2$. Set $q = 2^{n/2}$ and let $c \in \mathbb{F}_{2^n}$ and $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$. If the polynomial*

$$X^{2^i+1} + cX^{2^i} + c^qX + 1$$

is irreducible over $\mathbb{F}_{2^n}$, then the function

$$F(x) = x(x^{2^i} + x^q + cx^{2^iq}) + x^{2^i}(c^qx^q + sx^{2^iq}) + x^{(2^i+1)q}$$

is APN on $\mathbb{F}_{2^n}$.

It was checked with a computer that some of the functions of the present class and of the previous one are CCZ-inequivalent to power functions for $n = 6$. It remains open to prove the same property for every even $n \geq 6$.

Open problem: The APN power functions listed above are not permutations when n is even. The question of knowing whether there exist APN permutations when n is even was wide open until recently. This question was first raised (at least in a printed form) in [139]. We have seen that the answer is "no" for all plateaued functions (this was first observed in this same paper [139] when all the component functions of F are partially-bent; Nyberg generalized there a result given without a complete proof in [148], which was valid only for quadratic functions). We have also seen above in Subsection 3.1.4 that the answer is "no" for a class of functions including power functions. And X.-d. Hou proved in [108] that it is also "no" for those functions whose univariate representation coefficients lie in $\mathbb{F}_{2^{n/2}}$; he showed this problem is related to a conjecture on the symmetric group of $\mathbb{F}_{2^n}$. An example of APN permutation in 6 variables has been given by J. Dillon at last conference Fq 9 [80]. The existence of infinite classes of APN permutations when n is even remains open.

• We introduce now a method for constructing APN functions from bent functions, which leads to two classes (we do not know yet if these classes are new) and should lead to others. Let B be a bent $(n, n/2)$-function and let G be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n/2}$. Let

$$F : x \in \mathbb{F}_2^n \to (B(x), G(x)) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}.$$

F is APN if and only if, for every nonzero $a \in \mathbb{F}_2^n$, and for every $c \in \mathbb{F}_2^{n/2}$ and $d \in \mathbb{F}_2^{n/2}$, the system of equations

$$\left\{ \begin{array}{rcl} B(x) + B(x+a) & = & c \\ G(x) + G(x+a) & = & d \end{array} \right.$$

has 0 or 2 solutions.

Since B is bent, the number of solutions of the first equation equals $2^{n/2}$ for every $a \neq 0$. We need to find functions G such that, among these $2^{n/2}$ solutions, only 0 or 2 satisfy additionally the second equation.

Obviously, the condition on G depends on the choice of B. We take the Maiorana-McFarland function defined on $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ by $B(x, y) = xy$, where xy is the product of x and y in the field $\mathbb{F}_{2^{n/2}}$. We write then (a, b)

with $a, b \in \mathbb{F}_{2^{n/2}}$ instead of $a \in \mathbb{F}_2^n$. Changing c into $c + ab$, the system of equations above becomes

$$\begin{cases} bx + ay & = & c \\ G(x, y) + G(x + a, y + b) & = & d \end{cases}$$

It is straightforward to check that F is APN if and only if, for every nonzero ordered pair (a, b) in $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ and every c, d in $\mathbb{F}_{2^{n/2}}$, denoting $G_{a,b,c}(x) = G(ax, bx + c)$:

1. for every $y \in \mathbb{F}_{2^{n/2}}$, the function $x \in \mathbb{F}_{2^{n/2}} \to G(x, y)$ is APN (this condition corresponds to the case $b = 0$);

2. for every $x \in \mathbb{F}_{2^{n/2}}$, the function $y \in \mathbb{F}_{2^{n/2}} \to G(x, y)$ is APN (this condition corresponds to the case $a = 0$);

3. for every $(a, b) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ such that $a \neq 0$ and $b \neq 0$, and for every $c, d \in \mathbb{F}_{2^{n/2}}$, the equation $G_{a,b,c}(x) + G_{a,b,c}(x + 1) = d$ has 0 or 2 solutions.

Note that condition 3 is equivalent to "$G_{a,b,c}$ is APN", since for every nonzero $e \in \mathbb{F}_{2^{n/2}}$, we have $G_{ae,be,c}(x) + G_{ae,be,c}(x + 1) = G_{a,b,c}(ex) + G_{a,b,c}(ex + e)$, and therefore condition 3 includes condition 1 (which corresponds to $b = 0$). Note also that in condition 3, we can without loss of generality take $a = 1$. Moreover, if G is quadratic (that is, if F is quadratic) then since $G_{a,b,c}+G_{a,b,0}$ is affine, we can without loss of generality take $c = 0$.
Let us choose $G(x, y) = sx^{2^i+1} + ty^{2^i+1} + ux^{2^i}y + vxy^{2^i}$, where $(n/2, i) = 1$ and $s, t, u, v \in \mathbb{F}_{2^{n/2}}$, $s \neq 0$, $t \neq 0$. Then, since the Gold function x^{2^i+1} is APN, the function $x \in \mathbb{F}_{2^{n/2}} \to G(x, y)$ is APN for every $y \in \mathbb{F}_{2^{n/2}}$ (the other terms being affine in x) and the function $y \in \mathbb{F}_{2^{n/2}} \to G(x, y)$ is APN for every $x \in \mathbb{F}_{2^{n/2}}$. The function $G_{a,b,c}(x)$ equals $(sa^{2^i+1} + tb^{2^i+1} + ua^{2^i}b + vab^{2^i})\, x^{2^i+1}$, plus an affine function. Then, if the polynomial $sX^{2^i+1} + t + uX^{2^i} + vX$ has no zero in $\mathbb{F}_{2^{n/2}}$ (for instance if it is irreducible over $\mathbb{F}_{2^{n/2}}$), we have $sa^{2^i+1} + tb^{2^i+1} + ua^{2^i}b + vab^{2^i} \neq 0$ for every $a \neq 0$ and every $b \neq 0$ (dividing this expression by b^{2^i+1} and taking $X = a/b$), and the equation $G_{a,b,c}(x) + G_{a,b,c}(x + 1) = d$ has at most 2 solutions, since the function $x \to x^{2^i+1}$ is APN. Thus, F is then APN.
If we take for instance $G(x, y) = x^3 + xy^2 + y^3$ with $(n/2, 3) = 1$, then the polynomial above equals $X^3 + X + 1$ and has no zero (which implies that it is irreducible since it has degree 3), since $X^3 = X + 1$ implies $X^8 = X^2(X^2 + 1) = X(X^3 + X) = X$, which in its turn implies $X \in \mathbb{F}_2$, since $(n/2, 3) = 1$, and $X^3 + X + 1$ has no zero in $\mathbb{F}_2$. More generally than

X^3+X+1, if we take any irreducible polynomial over a subfield $\mathbb{F}_{2^r}$ of $\mathbb{F}_{2^{n/2}}$ which has the desired form $sX^{2^i+1}+t+uX^{2^i}+vX$, then its roots will belong to the field $\mathbb{F}_{2^{r(2^i+1)}}$ and if $gcd(n,2^i+1)=1$, then it will have no root in $\mathbb{F}_{2^{n/2}}$ since it has no root in $\mathbb{F}_{2^r}$ and $\mathbb{F}_{2^{r(2^i+1)}}\cap\mathbb{F}_{2^{n/2}}=\mathbb{F}_{2^r}$. When n is not divisible by 3, this works for instance with the polynomial $1+X+X^9$ (taking $r=1$ and $i=3$). For n divisible by 4 but not by 3, it works with any of the 20 irreducible polynomials of degree 3 over $\mathbb{F}_4$ (taking $r=2$; these polynomials can be obtained at URL http://www.theory.cs.uvic.ca/ cos/gen/poly.html). For n divisible by 4 but not by 5, it works with 23 polynomials of degree 5 (those of the desired form given by this same URL).
If we take $G(x,y)=x^{2^i+1}+\lambda\, y^{2^i+1}$ where $(i,n/2)=1$ and λ is not a cube (λ can exist only if $n/2$ is even, i.e. n is divisible by 4) then the polynomial equals $X^{2^i+1}+\lambda$. This polynomial has no zero since $gcd(2^n-1,2^i+1)=3$ and since λ is not a cube. The function is therefore APN.
- It is also easy to construct differentially 4-uniform functions this way. For instance the functions $(x,y)\rightarrow(xy,x^3+y^5)$, $(x,y)\rightarrow(xy,x^3+y^6)$ and $(x,y)\rightarrow(xy,x^5+y^6)$. More interestingly there are non-quadratic differentially 4-uniform functions: the function $(x,y)\rightarrow(xy,(x^3+w)(y^3+w'))$, where w and w' belong to $\mathbb{F}_{2^{n/2}}\setminus\{x^3,\ x\in\mathbb{F}_{2^{n/2}}\}$, with $n/2$ even (for allowing the existence of such elements), and $(x,y)\rightarrow(xy,x^3(y^2+y+1)+y^3)$, with $n/2$ odd (so that y^2+y+1 is never null).

Open problem: Find infinite classes of APN functions CCZ-inequivalent to power functions and to quadratic functions.
Observation: A classification under CCZ-inequivalence of all APN functions up to dimension five and a (non-exhaustive) list of CCZ-inequivalent functions in dimension 6 have been given in [21]. One of the functions in dimension 6 is CCZ-inequivalent to power functions and to quadratic functions, as proved by Edel and Pott in [94] (this had not been seen by the authors of [21]). This function is:

$$x^3+\alpha^{17}(x^{17}+x^{18}+x^{20}+x^{24})+tr_2(x^{21})+tr_3(\alpha^{18}x^9)$$
$$+\alpha^{14}\,tr_6\,(\alpha^{52}x^3+\alpha^6x^5+\alpha^{19}x^7+\alpha^{28}x^{11}+\alpha^2x^{13}).$$

Differentially 4-uniform functions Additionally to those listed above, such functions can be obtained from APN functions by adding a function taking its value in a pair (that is, up to translation, by adding a Boolean function times a nonzero vector), or composing it on the left with a 2-to-1 affine function. The Gold functions x^{2^i+1} such that $gcd(i,n)=$

2 are straightforwardly differentially 4-uniform and the Kasami functions $x^{2^{2i}-2^i+1}$ such that n is divisible by 2 but not by 4 and $gcd(i,n)=2$ are also differentially 4-uniform, as proved in [105]. The functions $ax^{2^{2s}+1}+bx^{2^s+1}+cx^{2^{2s}+2^s}$ such that $gcd(s,n)=1$ are also differentially 4-uniform when they are not APN, as shown in [14]. The functions $x^{2^{n-1}-1}+ax^5$ (n odd, $a \in \mathbb{F}_{2^n}$) and $x^{2^{n/2}+2^{n/4}+1}$ (n divisible by 4) are also differentially 4-uniform, as shown in the conference [19] (paper to appear). Some constructions of differentially 4-uniform functions have been given in [133], in connection with commutative semifields. A semifield is a finite algebraic structure $(E,+,\circ)$ such that (1) $(E,+)$ is an Abelian group, (2) the operation $\circ$ is distributive on the left and on the right with respect to $+$, (3) there is no nonzero divisor of 0 in E and (4) E contains an identity element with respect to $\circ$. This structure has been very useful for constructing planar functions in odd characteristic. In characteristic 2, it may lead to new APN functions by considering for instance the function $(x\circ x)\circ x$ in a classical semifield (there are two classes of them, whose underlying Abelian group is the additive group of $\mathbb{F}_{2^n}$: the Albert semifields, in which the multiplication is $x\circ y = xy+\beta(xy)^\sigma$, where $x \to x^\sigma$ is an automorphism of the field $\mathbb{F}_{2^n}$ which is not a generator and $\beta \notin \{x^{\sigma+1};\, x\in\mathbb{F}_{2^n}\}$, and the Knuth semifield where the multiplication is $x\circ y = xy+(xtr(y)+ytr(x))^2$, where tr is a trace function from $\mathbb{F}_{2^n}$ to a suitable subfield).

More open problems:

1. Find secondary constructions of APN and AB functions.

2. Derive more constructions of APN/AB functions from perfect nonlinear functions, and *vice versa*.

3. Classify APN functions, or at least their extended Walsh spectra, or at least their nonlinearities.
Observations:
For n odd, the known APN functions have three possible spectra:

- the spectrum of the AB functions which gives a nonlinearity of $2^{n-1}-2^{\frac{n-1}{2}}$,
- the spectrum of the inverse function, which takes any value divisible by 4 in $[-2^{n/2+1}+1; 2^{n/2+1}+1]$ and gives a nonlinearity close to $2^{n-1}-2^{n/2}$,

- the spectrum of the Dobbertin function which is more complex (it is divisible by $2^{n/5}$ and not divisible by $2^{2n/5+1}$); its nonlinearity seems to be bounded below by approximately $2^{n-1} - 2^{3n/5-1} - 2^{2n/5-1}$ - maybe equal - but this has to be proven (or disproven).

For n even, the spectra may be more diverse:

- the Gold functions whose component functions are bent for a third of them and have nonlinearity $2^{n-1} - 2^{n/2}$ for the rest of them; the Kasami functions which have the same extended spectra,
- the Dobbertin function (same observation as above),
- As soon as $n \geq 6$, we find (quadratic) functions with different spectra.

The nonlinearities seem also bounded below by approximately $2^{n-1} - 2^{3n/5-1} - 2^{2n/5-1}$ (but this has to be proven ... or disproven too). Note that the question of classifying APN functions is open even when restricting ourselves to quadratic APN functions (even classifying their Walsh spectra is open for even numbers of variables). Already for $n = 6$ there are at least 9 mutually CCZ-inequivalent quadratic APN polynomials which are CCZ-inequivalent to power functions [23].
Open question: The nonlinearities of the known APN functions do not seem to be very weak; is this situation general to all APN functions or specific to the APN functions found so far?

Observation: We have seen in Proposition 13 that an APN function cannot have null nonlinearity. We can improve upon this lower bound under some hypothesis:

Proposition 24 *[54] Let F be an APN function in $n > 2$ variables. For all real numbers a and b such that $a \leq b$, let $N_{a,b}$ be the number of ordered pairs $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^{n*}$ such that $\widehat{1_{G_F}}^2(u, v) \in]2^n + a; 2^n + b[$, where $\widehat{1_{G_F}}(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}$. Then:*

$$nl(F) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{1}{2}(b + a + \sqrt{\Delta_{a,b}})},$$

where $\Delta_{a,b} = (N_{a,b} + 1)(b - a)^2 + a\,b\,2^{n+2}(2^n - 1) + 2^{4n+2} - 2^{3n+2}$.

Proof: Relation (13) shows that for all real numbers a, b we have

$$\sum_{\substack{u \in \mathbb{F}_2^n, \\ v \in \mathbb{F}_2^{n*}}} (\widehat{1_{G_F}}^2(u, v) - 2^n - a)(\widehat{1_{G_F}}^2(u, v) - 2^n - b) = (2^{3n} + a\,b\,2^n)(2^n - 1), \quad (16)$$

since $\sum_{u\in\mathbb{F}_2^n,v\in\mathbb{F}_2^{n*}}(\widehat{1_{G_F}}^2(u,v)-2^n)=0$ and $\sum_{u\in\mathbb{F}_2^n,v\in\mathbb{F}_2^{n*}}(\widehat{1_{G_F}}^2(u,v)-2^n)^2 = \sum_{u\in\mathbb{F}_2^n,v\in\mathbb{F}_2^{n*}}\widehat{1_{G_F}}^2(u,v)(\widehat{1_{G_F}}^2(u,v)-2^{n+1})+2^{3n}(2^n-1)$.
The expression $(x-a)(x-b)$ is non-negative outside $]a,b[$; it takes its minimum at $x=\frac{b+a}{2}$ and this minimum equals $-\frac{(b-a)^2}{4}$. We deduce that we have $(\widehat{1_{G_F}}^2(u,v)-2^n-a)(\widehat{1_{G_F}}^2(u,v)-2^n-b)\geq -\frac{(b-a)^2}{4}$ for these $N_{a,b}$ ordered pairs and $(\widehat{1_{G_F}}^2(u,v)-2^n-a)(\widehat{1_{G_F}}^2(u,v)-2^n-b)\geq 0$ for all the others. Hence $-\frac{(b-a)^2}{4}\leq(\widehat{1_{G_F}}^2(u,v)-2^n-a)(\widehat{1_{G_F}}^2(u,v)-2^n-b)\leq 2^{4n}-2^{3n}+a\,b\,2^n(2^n-1)+N_{a,b}\frac{(b-a)^2}{4}$ for any $(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^{n*}$, that is, $(\widehat{1_{G_F}}^2(u,v)-2^n)^2-(b+a)(\widehat{1_{G_F}}^2(u,v)-2^n)+ab-(2^{4n}-2^{3n}+a\,b\,2^n(2^n-1)+N_{a,b}\frac{(b-a)^2}{4})\leq 0$, which implies

$$\frac{1}{2}\left(b+a-\sqrt{\Delta_{a,b}}\right)\leq\widehat{1_{G_F}}^2(u,v)-2^n\leq\frac{1}{2}\left(b+a+\sqrt{\Delta_{a,b}}\right),$$

where $\Delta_{a,b}=(b+a)^2-4(a\,b-2^{4n}+2^{3n}-a\,b\,2^n(2^n-1)-N_{a,b}\frac{(b-a)^2}{4})=(N_{a,b}+1)(b-a)^2+a\,b\,2^{n+2}(2^n-1)+2^{4n+2}-2^{3n+2}$. This implies that the nonlinearity of F is bounded below by

$$2^{n-1}-\frac{1}{2}\sqrt{2^n+\frac{1}{2}\left(b+a+\sqrt{\Delta_{a,b}}\right)}.$$

□

Consequences:
- taking $b=-a=2^n$, we see that if $\widehat{1_{G_F}}^2(u,v)$ does not take values in the range $]0;2^{n+1}[$, then F is AB (this was known according to Relation (13)).
- more generally, taking $a=-\frac{2^{2n}}{b}$ (b necessarily greater than or equal to 2^n since we shall see below that otherwise this would contradict the Sidelnikov-Chabaud-Vaudenay bound), we see that if $\widehat{1_{G_F}}^2(u,v)$ does not take values in the range $]2^n-\frac{2^{2n}}{b};2^n+b[$, the nonlinearity of F is bounded below by $2^{n-1}-\frac{1}{2}\sqrt{2^n+b}$. For instance (for $b=2^{n+1}$), if $\widehat{1_{G_F}}^2(u,v)$ does not take values in the range $]2^{n-1};3\cdot 2^n[$, the nonlinearity of F is bounded below by $2^{n-1}-\frac{1}{2}\sqrt{3\cdot 2^n}$.

As observed by G. Leander (private communication), if n is odd and F is an APN power (n,n)-function, then since we know that F is a bijection and thus all functions $v\cdot F$ have the same Walsh spectrum, we have, according to Relation (12):

$$\max_{v\neq 0,u} \widehat{1_{G_F}}^4(u,v) \leq \frac{\sum_{v\neq 0,u} \widehat{1_{G_F}}^4(u,v)}{2^n-1} = 2^{3n+1}.$$

Thus we have $\max_{v\neq 0,u} |\widehat{1_{G_F}}(u,v) \leq 2^{\frac{3n+1}{4}}$ and

$$nl(F) \geq 2^{n-1} - 2^{\frac{3n-3}{4}}. \tag{17}$$

In fact, the lower bound of Proposition 24 can be improved then: denoting by $N'_{a,b}$ the number $\frac{N_{a,b}}{2^n-1}$ of elements u of $\mathbb{F}_2^n$ such that $\widehat{1_{G_F}}^2(u,v) \in]2^n{+}a; 2^n{+}b[$ (which is the same for every $v \in \mathbb{F}_2^{n*}$), we have:

$$nl(F) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{1}{2}\left(b + a + \sqrt{\Delta'_{a,b}}\right)},$$

where $\Delta'_{a,b} = (N'_{a,b}+1)(b-a)^2 + a\,b\,2^{n+2} + 2^{3n+2}$. This does not improve the lower bound in the cases considered above but it does in general. Note that, for $a = b = -2^n$, it gives (17).

Concluding remark.
As we can see, very few functions usable as S-boxes have emerged so far. The Gold functions, all the other recently found quadratic functions and the Welch functions have too low algebraic degrees for being widely chosen for the design of new S-boxes. The Kasami functions themselves seem too closely related to quadratic functions. The inverse function has many very nice properties: large Walsh spectrum and good nonlinearity, differential uniformity of order at leat 4, fast implementation. But it has a potential weakness, which did not lead yet to efficient attacks, but may in the future: denoting its input by x and its output by y, the bilinear expression xy equals 1 for every nonzero x. The candidates for future block ciphers not using the inverse function as an S-box are the Niho and Dobbertin functions. The Niho functions exist only in odd numbers of variables (which is not convenient for implementation in software, but is not a real problem in hardware), and the Dobbertin function needs n to be divisible by 5 (idem). The nonlinearity is also a concern. So further studies seem indispensable for the future designs of SP networks. This is the main open problem.

3.1.8 Lower bounds on the nonlinearity of S-boxes by means of their algebraic immunity

As proved in [53], Lobanov's bound recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" for Boolean functions generalizes to (n, m)-functions as follows:

$$nl(F) \geq 2^m \sum_{i=0}^{AI(F)-2} \binom{n-1}{i},$$

where $AI(f)$ is the basic algebraic immunity of F.
Note that, applying Lobanov's bound to the component functions of F, we obtain

$$nl(F) \geq 2 \sum_{i=0}^{AI_{comp}(F)-2} \binom{n-1}{i},$$

where $AI_{comp}(F)$ is the component algebraic immunity of F. The inequality $AI_{comp}(F) \geq AI_{gr}(F) - 1$ implies then

$$nl(F) \geq 2 \sum_{i=0}^{AI_{gr}(F)-3} \binom{n-1}{i},$$

where $AI_{gr}(F)$ is the graph algebraic immunity of F.

3.2 Higher order nonlinearities

For every positive integer r, the r-th order nonlinearity of a vectorial function F is the minimum r-th order nonlinearity of its component functions (recall that, as defined in the previous chapter, the r-th order nonlinearity of a Boolean function equals its minimum Hamming distance to functions of algebraic degrees at most r). As proved in [53], the bounds recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" for Boolean functions generalize to (n, m)-functions as follows:

$$nl_r(F) \geq 2^m \sum_{i=0}^{AI(F)-r-1} \binom{n-r}{i}$$

and

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

(the first of these two bounds can be slightly improved as for Boolean functions).

Applying the bounds valid for Boolean functions to the component functions of F, we have also:

$$nl_r(F) \geq 2 \sum_{i=0}^{AI_{comp}(F)-r-1} \binom{n-r}{i}$$

and

$$nl_r(F) \geq \sum_{i=0}^{AI_{comp}(F)-r-1} \binom{n}{i} + \sum_{i=AI_{comp}(F)-2r}^{AI_{comp}(F)-r-1} \binom{n-r}{i}.$$

The inequality $AI_{comp}(F) \geq AI_{gr}(F) - 1$ implies then

$$nl_r(F) \geq 2 \sum_{i=0}^{AI_{gr}(F)-r-2} \binom{n-r}{i}$$

and

$$nl_r(F) \geq \sum_{i=0}^{AI_{gr}(F)-r-2} \binom{n}{i} + \sum_{i=AI_{gr}(F)-2r-1}^{AI_{gr}(F)-r-2} \binom{n-r}{i}.$$

In the definition of $nl_r(F)$, we consider approximations by Boolean functions of algebraic degrees at most r of the component functions of F, that is, of the functions equal to F composed on the left by nonzero linear Boolean functions on $\mathbb{F}_2^m$ (and taking instead non-constant affine functions does not change the value). We can also consider F composed by functions of higher degrees:

Definition 12 *For every S-box $F : F_2^n \to \mathbb{F}_2^m$, for every positive integers $s \leq m$ and $t \leq n+m$, and every non-negative integer $r \leq n$, we define:*

$$\begin{aligned} nl_{s,r}(F) &= \min\{nl_r(f \circ F);\ f \in \mathcal{B}_m,\ d^\circ f \leq s,\ f \neq cst\} \\ &= \min\{d_H(g, f \circ F);\ f \in \mathcal{B}_m,\ d^\circ f \leq s,\ f \neq cst,\ g \in \mathcal{B}_n,\ d^\circ g \leq r\} \end{aligned}$$

and

$$NL_t(F) = \min\{w_H(h(x, F(x)));\ h \in \mathcal{B}_{n+m},\ d^\circ h \leq t,\ h \neq cst\},$$

where d_H denotes the Hamming distance and $\mathcal{B}_m$ the set of m-variable Boolean functions, as in the previous chapter.

Definition 12 excludes obviously $f = cst$ and $h = cst$ because the knowledge of the distance $d_H(g, f \circ F)$ or of the weight $w_H(h(x, F(x)))$ when f or h is constant gives no information specific to F and usable in an attack against a stream or block cryptosystem using F as an S-box.
Clearly, for every S-box F and every integers $t \leq t'$, $s \leq s'$ and $r \leq r'$, we have $NL_t(F) \geq NL_{t'}(F)$ and $nl_{s,r}(F) \geq nl_{s',r'}(F)$. Note also that, for every vectorial function F, we have $NL_1(F) = nl(f)$.
T. Shimoyama and T. Kaneko have exhibited in [149] several quadratic functions h and pairs (f, g) of quadratic functions showing that the nonlinearities NL_2 and $nl_{2,2}$ of some sub-S-boxes of the DES are null (and therefore that the global S-box of each round of the DES has the same property). They deduced a "higher-order non-linear" attack (an attack using the principle of the linear attack by Matsui but with non-linear approximations) which needs 26% less data than Matsui's attack. This improvement is not very significant, practically, but some recent studies, not yet published, seem to show that the notions of NL_t and $nl_{s,r}$ can be related to potentially more powerful attacks. Note that we have $NL_{\max(s,r)}(F) \leq nl_{s,r}(F)$ by taking $h(x, y) = g(x) + f(y)$ (since $f \neq cst$ implies then $h \neq cst$) and the inequality can be strict if $s > 1$ or $r > 1$ since a function $h(x, y)$ of low degree and such that $w_H(h(x, F(x)))$ is small can exist while no such function exists with separated variables x and y, that is, of the form $g(x) + f(y)$. This is the case, for instance, of the S-box of the AES for $s = 1$ and $r = 2$ (see below).

We now study bounds on these parameters. We begin with an easy one coming from the existence of n-variable Boolean functions of algebraic degree s and Hamming weight 2^{n-s}:

Proposition 25 *[53] For every positive integers m, n, $s \leq m$ and $r \leq n$ and every (n, m)-function F, we have: $NL_s(F) \leq 2^{n-s}$ and $nl_{s,r}(F) \leq 2^{n-s}$. These inequalities are strict if F is not balanced (that is, if its output is not uniformly distributed over $\mathbb{F}_2^m$).*

The bound $nl_{s,r}(F) \leq 2^{n-s}$ is asymptotically almost tight (in a sense which will be precised in Proposition 27) for permutations when $r \leq s \leq .227\, n$.

3.2.1 Existence of permutations with lower bounded higher order nonlinearities

Proposition 26 *[53] Let n and s be positive integers and let r be a non-negative integer. Let D be the greatest integer such that*

$$\sum_{t=0}^{D} \binom{2^n}{t} \leq \frac{\binom{2^n}{2^{n-s}}}{2^{\sum_{i=0}^{s}\binom{n}{i} + \sum_{i=0}^{r}\binom{n}{i}}}.$$

There exist (n,n)-permutations F whose higher order nonlinearity $nl_{s,r}(F)$ is strictly greater than D.

Proof. For every integers $i \in [0, 2^n]$ and r, let us denote by $A_{r,i}$ the number of codewords of Hamming weight i in the Reed-Muller code of order r. Given a number D, a permutation F and two Boolean functions f and g, if we have $d_H(f \circ F, g) \leq D$ then F^{-1} maps the support $supp(f)$ of f onto the symmetric difference $supp(g)\Delta E$ between $supp(g)$ and a set E of size at most D (equal to the symmetric difference between $F^{-1}(supp(f))$ and $supp(g)$). And F^{-1} maps $\mathbb{F}_2^n \setminus supp(f)$ onto the symmetric difference between $\mathbb{F}_2^n \setminus supp(g)$ and E. Given f, g and E and denoting by i the size of $supp(f)$ (with $0 < i < 2^n$, since $f \neq cst$), the number of permutations whose restriction to $supp(g)\Delta E$ is a one-to-one function onto $supp(f)$ and whose restriction to $(\mathbb{F}_2^n \setminus supp(g))\Delta E$ is a one-to-one function onto $\mathbb{F}_2^n \setminus supp(f)$ equals $i!\,(2^n - i)!$. We deduce that the number of permutations F such that $nl_{s,r}(F) \leq D$ is bounded above by

$$\sum_{t=0}^{D} \binom{2^n}{t} \sum_{0<i<2^n} \sum_{j=1}^{2^n} A_{s,i} A_{r,j}\, i!\,(2^n - i)!$$

Since the non-constant codewords of the Reed-Muller code of order s have weights between 2^{n-s} and $2^n - 2^{n-s}$, we deduce that the probability $P_{s,r,D}$ that a permutation F chosen at random (with uniform probability) satisfies $nl_{s,r}(F) \leq D$ is bounded above by

$$\sum_{t=0}^{D} \binom{2^n}{t} \sum_{j=0}^{2^n} A_{r,j} \sum_{2^{n-s} \leq i \leq 2^n - 2^{n-s}} A_{s,i} \frac{i!\,(2^n - i)!}{2^n!} =$$

$$\sum_{t=0}^{D} \binom{2^n}{t} \sum_{j=0}^{2^n} A_{r,j} \sum_{2^{n-s} \leq i \leq 2^n - 2^{n-s}} \frac{A_{s,i}}{\binom{2^n}{i}}$$

$$< \frac{\left(\sum_{t=0}^{D} \binom{2^n}{t}\right) 2^{\sum_{i=0}^{s} \binom{n}{i} + \sum_{i=0}^{r} \binom{n}{i}}}{\binom{2^n}{2^{n-s}}}. \tag{18}$$

If this upper bound is at most 1, then we deduce that $P_{s,r,D} < 1$ and this proves that there exist permutations F from $\mathbb{F}_2^n$ to itself whose higher order nonlinearity $nl_{s,r}(F)$ is strictly greater than D. This completes the proof.□

Let us see now what happens when n tends to ∞. Let $H_2(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ be the binary entropy function.

Proposition 27 *[53] Let $\frac{s_n}{n}$ tend to a limit $\rho \leq .227$ when n tends to ∞. If $r_n \leq \mu\, n$ for every n, where $1 - H_2(\mu) > \rho$ (e.g. if r_n/s_n tends to a limit strictly smaller than 1), then for every $\rho' > \rho$, almost all permutations F of $\mathbb{F}_2^n$ satisfy $nl_{s_n,r_n}(F) \geq 2^{(1-\rho')n}$.*

Proof. We know (see e.g. [130], page 310) that, for every integer n and every $\lambda \in [0, 1/2]$, we have $\sum_{i \leq \lambda n} \binom{n}{i} \leq 2^{nH_2(\lambda)}$. According to the Stirling formula, we have also, when i and j tend to ∞: $i! \sim i^i e^{-i}\sqrt{2\pi i}$ and $\binom{i+j}{i} \sim \frac{(\frac{i+j}{i})^i (\frac{i+j}{j})^j}{\sqrt{2\pi}} \sqrt{\frac{i+j}{ij}}$. For $i + j = 2^n$ and $i = 2^{n-s_n}$, this gives

$$\begin{aligned}\binom{2^n}{2^{n-s_n}} &\sim \frac{(2^{s_n})^{2^{n-s_n}}}{\sqrt{2\pi}(1-2^{-s_n})^{2^n - 2^{n-s_n}}} \sqrt{\frac{2^{s_n}}{2^n - 2^{n-s_n}}} \\ &= \frac{2^{s_n 2^{n-s_n}}}{\sqrt{2\pi}\, 2^{(2^n - 2^{n-s_n})\ln(1-2^{-s_n})\log_2 e}} \sqrt{\frac{2^{s_n}}{2^n - 2^{n-s_n}}}.\end{aligned}$$

We deduce then from Inequality (18):

$$\log_2 P_{s_n,r_n,D_n} = O\left(2^n \left[H_2\left(\frac{D_n}{2^n}\right) + 2^{-n(1-H_2(s_n/n))} + 2^{-n(1-H_2(r_n/n))} \right.\right.$$
$$\left.\left. -2^{-s_n + \log_2(s_n)} - 2^{-s_n}(1-2^{-s_n})\log_2 e\right]\right)$$

(we omit $-\frac{s_n}{2^{n+1}} + \frac{n}{2^{n+1}}\log_2(1-2^{-s_n})$ inside the brackets above since it is negligible).
For $\rho \leq .227$, we have $1 - H_2(\rho) > \rho$. If $\lim \frac{s_n}{n} = \rho \leq .227$ then there exists $\rho' > \rho$ such that $1 - H_2(\rho') > \rho'$ and such that asymptotically we have $s_n \leq \rho'\, n$; hence $2^{-n(1-H_2(s_n/n))}$ is negligible with respect to 2^{-s_n}. And if $r_n \leq \mu\, n$ where $1 - H_2(\mu) > \rho$, then we have $2^{-n(1-H_2(r_n/n))} = o(2^{-s_n})$ and for $D_n = 2^{(1-\rho')n}$ where ρ' is any number strictly greater than ρ, we have $H_2\left(\frac{D_n}{2^n}\right) = H_2\left(2^{-\rho'\, n}\right) = \rho'\, n\, 2^{-\rho'\, n} - (1 - 2^{-\rho'\, n})\log_2(1 - 2^{-\rho'\, n}) = o(2^{-\rho\, n}) = o(2^{-s_n})$. We obtain that, asymptotically, $nl_{s_n,r_n}(F) > 2^{(1-\rho')n}$ for every $\rho' > \rho$. □

3.2.2 The inverse S-box

For $F_{inv}(x) = x^{2^n-2}$ and $f_{inv}(x) = tr_n(F_{inv}(x))$, we have $nl_r(F_{inv}) = nl_r(f_{inv})$ as for any power permutation. Recall that, for $r = 1$, this parameter equals $2^{n-1} - 2^{n/2}$ when n is even and is close to this number when n is odd, and that for $r > 1$, it is approximately bounded below by

$2^{n-1} - 2^{(1-2^{-r})\,n}$ (see more in [52]). We have $NL_2(F_{inv}) = 0$, since we have $w_H(h(x, F_{inv}(x))) = 0$ for the bilinear function $h(x,y) = tr_n(axy)$ where a is any nonzero element of null trace and xy denotes the product of x and y in $\mathbb{F}_{2^n}$. Indeed we have $x\,F_{inv}(x) = 1$ for every nonzero x. As observed in [73], we have also $w_H(h(x, F_{inv}(x))) = 0$ for the bilinear functions $h(x,y) = tr_n(a(x + x^2y))$ and $h(x,y) = tr_n(a(y + y^2x))$ where a is now any nonzero element, and for the quadratic functions $h(x,y) = tr_n(a(x^3 + x^4y))$ and $h(x,y) = tr_n(a(y^3 + y^4x))$. These properties are the core properties used in the tentative algebraic attack on the AES by Courtois and Pieprzyk [73].

It is proved in [53] that, for every ordered pair (s,r) of strictly positive integers, we have:

- $nl_{s,r}(F_{inv}) = 0$ if $r + s \geq n$;
- $nl_{s,r}(F_{inv}) > 0$ if $r + s < n$;

and that, in particular, for every ordered pair (s,r) of positive integers such that $r + s = n - 1$, we have $nl_{s,r}(F_{inv}) = 2$. The other values are unknown when $r + s < n$, except for small values of n.

3.3 Nonlinearity of S-boxes in stream ciphers

The classical notion of nonlinearity (see Definition 5) and its generalizations given in Subsection 3.2 have been introduced in the framework of block ciphers: due to the iterative structure of these ciphers, the knowledge of a nonlinear combination by a function f of the output bits of an S-box F, such that $f \circ F$ has a low (higher order) nonlinearity, does not necessarily lead to an attack, unless the degree of f is low. This is why, in Definition 12, the degree of f is also specified. We recall in Figures 2 and 3 below how vectorial functions can be used in the pseudo-random generators of stream ciphers to speed up the ciphers.

Since the structure of these pseudo-random generators is not iterative, all of the m binary sequences produced by an (n,m)-function can be combined by a linear or nonlinear (but non-constant) m-variable Boolean function f to perform (fast) correlation attacks. Consequently, a second generalization to (n,m)-functions of the notion of nonlinearity has been introduced (in [62], but the definition was based on the observations of Zhang and Chan in [162]).

Definition 13 *Let F be an (n,m)-function. The* unrestricted nonlinearity *$unl(F)$ of F is the minimum Hamming distance between all non-constant*

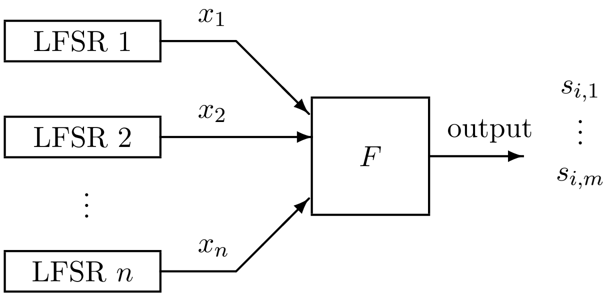

Figure 2: Combiner model

affine functions and all Boolean functions $g \circ F$, where g is any non-constant Boolean function on m variables.

If $unl(F)$ is small, then one of the linear or nonlinear (non-constant) combinations of the output bits to F has high correlation to a non constant affine function of the input, and a (fast) correlation attack is feasible.

Remark.
1. In Definition 13, the considered affine functions are non-constant, because the minimum distance between all Boolean functions $g \circ F$ (g non-constant) and all constant functions equals $\min_{b\in\mathbb{F}_2^m} |F^{-1}(b)|$ (each number $|F^{-1}(b)|$ is indeed equal to the distance between the null function and $g \circ F$, where g equals the indicator of the singleton $\{b\}$); it is therefore an indicator of the balancedness of F. It is bounded above by 2^{n-m} (and it equals 2^{n-m} if and only if F is balanced).
2. We can replace "non constant affine functions" by "nonzero linear functions" in the statement of Definition 13 (replacing g by $g \oplus 1$, if necessary).
3. Thanks to the fact that the affine functions considered in Definition 13 are non-constant, we can relax the condition that g is non-constant: the distance between a constant function and a non-constant affine function equals 2^{n-1}, and $unl(F)$ is clearly always smaller than 2^{n-1}.

The unrestricted nonlinearity of any (n,m)-function F is obviously unchanged when F is right-composed with an affine invertible mapping. Moreover, if A is a surjective linear (or affine) function from $\mathbb{F}_2^p$ (where p is some positive integer) into $\mathbb{F}_2^n$, then it is easily shown that $unl(F \circ A) = 2^{p-n}unl(F)$. Also, for every (m,p)-function ϕ, we have $unl(\phi \circ F) \geq unl(F)$ (indeed, the set $\{g\circ\phi,\ g \in \mathcal{BF}_p\}$, where $\mathcal{BF}_p$ is the set of p-variable Boolean

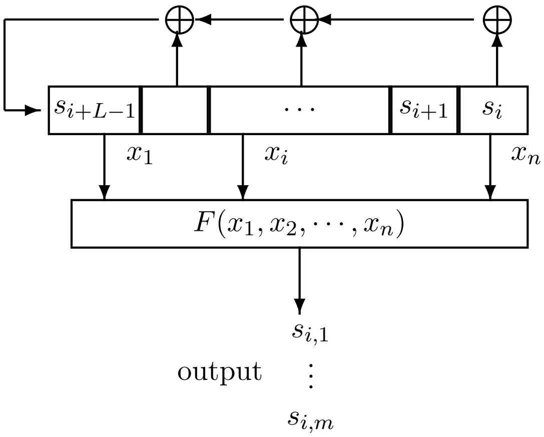

Figure 3: Filter model

functions, is included in $\mathcal{BF}_m$), and if ϕ is a permutation on $\mathbb{F}_2^m$, then we have $unl(\phi \circ F) = unl(F)$ (by applying the inequality above to $\phi^{-1} \circ F$).

A further generalization of the Zhang-Chan attack, called the *generalized correlation attack* has been introduced in [59]: considering implicit equations which are linear in the input variable x and of any degree in the output variable $z = F(x)$, the following probability is considered, for any non-constant function g and every functions $w_i : \mathbb{F}_2^m \to \mathbb{F}_2$:

$$Pr\,[g(z) + w_1(z)\,x_1 + w_2(z)\,x_2 + \cdots + w_n(z)\,x_n = 0], \qquad (19)$$

where $z = F(x)$ and where x uniformly ranges over $\mathbb{F}_2^n$.
The knowledge of such approximation g with a probability significantly higher than $1/2$ leads to an attack, because $z = F(x)$ corresponding to the output keystream is known, and therefore $g(z)$ and $w_i(z)$ are known for all $i = 1, \ldots, n$.
This led to a new notion of generalized nonlinearity:

Definition 14 *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. The* generalized Hadamard transform *$\hat{F} : (\mathbb{F}_2^{2^m})^{n+1} \to \mathbb{R}$ is defined as:*

$$\hat{F}(g(\cdot), w_1(\cdot), \ldots, w_n(\cdot)) = \sum_{x \in \mathbb{F}_2^n} (-1)^{g(F(x)) + w_1(F(x))\,x_1 + \cdots + w_n(F(x))\,x_n},$$

where the input is an $(n+1)$*-tuple of Boolean functions* $g, w_i : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$, $i = 1, \ldots, n$.
Let $\mathcal{W}$ *be the set of all* n*-tuple functions* $w(\cdot) = (w_1(\cdot), \ldots, w_n(\cdot))$*, where* w_i *is an* m*-variable Boolean function and such that* $w(z) = (w_1(z), \ldots, w_n(z)) \neq (0, \ldots, 0)$ *for all* $z \in \mathbb{F}_2^m$.
The generalized nonlinearity *is defined as:*

$$gnl(F) = \min\{\min_{0 \neq u \in \mathbb{F}_2^m} (w_H(u \cdot F), 2^n - w_H(u \cdot F)), nonlin_{gen}F\},$$

where

$$nonlin_{gen}F = 2^{n-1} - \frac{1}{2} \max_{g \in \mathcal{G}, w \in \mathcal{W}} \hat{F}(g(\cdot), w_1(\cdot), \ldots, w_n(\cdot)). \tag{20}$$

The generalized nonlinearity is clearly not greater than the other nonlinearity measures and provides linear approximations with better bias for (fast) correlation attacks.

3.3.1 Relations to the Walsh transforms and lower bounds

The unrestricted nonlinearity of F can be related to the values of the discrete Fourier transforms of the functions φ_b, and a lower bound (observed in [162]) depending on $nl(F)$ can be directly deduced:

Proposition 28 *For every* (n,m)*-function, we have*

$$unl(F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^{n*}} \sum_{b \in \mathbb{F}_2^m} \left|\widehat{\varphi_b}(u)\right|, \tag{21}$$

and:

$$unl(F) \geq 2^{n-1} - 2^{m/2} \left(2^{n-1} - nl(F)\right). \tag{22}$$

The lower bound (22) is far from giving a good idea of the best possible unrestricted nonlinearities: even if $nl(F)$ is close to the nonlinearity of bent functions, that is $2^{n-1} - 2^{n/2-1}$, it implies that $unl(F)$ is approximately greater than $2^{n-1} - 2^{\frac{n+m}{2}-1}$, whereas there exist balanced $(n, n/2)$-functions F such that $unl(F) = 2^{n-1} - 2^{n/2}$ (see below).

Proposition 29 *[59] Let* $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ *and let* $w(\cdot)$ *denote the* n*-tuple of* m*-bit Boolean functions* $(w_1(\cdot), \ldots, w_n(\cdot))$*. Then*

$$\begin{aligned} nonlin_{gen}F &= 2^{n-1} - 1/2 \sum_{z \in \mathbb{F}_2^m} \max_{w(z) \in \mathbb{F}_2^n - \{0\}} |\widehat{\varphi_b}(w(z))| \\ &= 2^{n-1} - \frac{1}{2^{m+1}} \sum_{z \in \mathbb{F}_2^m} \max_{\substack{0 \neq w(z) \in \\ \mathbb{F}_2^n}} \left| \sum_{v \in \mathbb{F}_2^m} (-1)^{v \cdot z} \widehat{1_{G_F}}(w(z), v) \right|, \end{aligned}$$

where $\widehat{1_{G_F}}$ denotes the Walsh transform. Hence

$$gnl(F) \geq 2^{n-1} - (2^m - 1)\left(2^{n-1} - nl(F)\right).$$

3.3.2 Upper bounds

If F is balanced, the minimum distance between the component functions $v \cdot F$ and the affine functions can not be achieved by constant affine functions, because $v \cdot F$, which is a Boolean balanced function, has distance 2^{n-1} to constant functions. Hence:

Proposition 30 (covering radius bound) *For every balanced S-box F, we have:*

$$unl(F) \leq nl(F). \tag{23}$$

This implies $unl(F) \leq 2^{n-1} - 2^{n/2-1}$.

Another upper bound:

$$unl(F) \leq 2^{n-1} - \frac{1}{2}\left(\frac{2^{2m} - 2^m}{2^n - 1} + \sqrt{\frac{2^{2n} - 2^{2n-m}}{2^n - 1} + \left(\frac{2^{2m} - 2^m}{2^n - 1} - 1\right)^2} - 1\right)$$

has been obtained in [62]. It improves upon the covering radius bound only for $m \geq n/2 + 1$, and the question of knowing whether it is possible to improve upon the covering radius bound for $m \leq n/2$ is open. In any case, this improvement will not be dramatic, at least for $m = n/2$, since it is shown (by using Relation (21)) in this same paper that the balanced function $F(x,y) = \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ x & \text{if } y = 0 \end{cases}$ satisfies $unl(F) = 2^{n-1} - 2^{n/2}$ (see other examples of S-boxes in [116], whose unrestricted nonlinearities seem low, however). It is pretty astonishing that an S-box with such high unrestricted nonlinearity exists; but it can be shown that this balanced function does not contribute to a good resistance to algebraic attacks and has null generalized nonlinearity (see below).

Proposition 31 *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then the following inequality holds.*

$$nonlin_{gen}F \leq 2^{n-1} - \frac{1}{4}\sum_{z \in \mathbb{F}_2^m} \sqrt{\frac{2^{n+2}|F^{-1}(z)| - 4|F^{-1}(z)|^2}{2^n - 1}}.$$

Furthermore if $F(x)$ is balanced, then we have:

$$gnl(F) \leq 2^{n-1} - 2^{n-1}\sqrt{\frac{2^m - 1}{2^n - 1}}$$

This upper bound is much lower than the covering radius bound $2^{n-1} - 2^{n/2-1}$ and than the upper bound given above for UN_F.

It is proved in [60] that the balanced function $F(x,y) = \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ x & \text{if } y = 0 \end{cases}$ has null generalized nonlinearity. Hence, a vectorial function may have very high unrestricted nonlinearity and have zero generalized nonlinearity. Some functions with good generalized nonlinearity are given in [60]:

1. $F(x) = tr_{n/m}(x^k)$ where $k = 2^i + 1$, $\gcd(i,n) = 1$, is a Gold exponent;

2. $F(x) = tr_{n/m}(x^k)$ where $k = 2^{2i} - 2^i + 1$ is a Kasami exponent such that $3i \equiv 1$ [mod] n,

where m divides n and n is odd, and where $tr_{n/m}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, have generalized nonlinearity satisfying $gnl(F) \geq 2^{n-1} - 2^{(n-1)/2+m-1}$.

4 Resilient vectorial Boolean functions

Resilient Boolean functions have been studied in the chapter "Boolean Functions for Cryptography and Error Correcting Codes". The notion, when extended to vectorial functions, is relevant, in cryptology, to quantum cryptographic key distribution [5] and to pseudo-random sequence generation for stream ciphers.

Definition 15 *Let n and m be two positive integers. Let t be an integer such that $0 \leq t \leq n$. An (n,m)-function $F(x)$ is called t-th order* correlation-immune *if its output distribution does not change when at most t coordinates x_i of x are kept constant. It is called t*-resilient *if it is balanced and t-th order correlation-immune, that is if it stays balanced when at most t coordinates x_i of x are kept constant*

This notion has a relationship with another notion which plays also a role in cryptography: an (n,m)-function F is called a *multipermutation* (see [154]) if any two ordered pairs $(x, F(x))$ and $(x', F(x'))$, such that x, $x' \in \mathbb{F}_2^n$ are distinct, differ in at least $m+1$ distinct positions (that is, collide in at most $n-1$ positions); such (n,m)-function ensures then a perfect diffusion; an (n,m)-function is a multipermutation if and only if the indicator of its graph $\{(x, F(x));\ x \in \mathbb{F}_2^n\}$ is an n-th order correlation-immune Boolean function (see [38]).

Since S-boxes must be balanced, we shall focus on resilient functions, but most of the results below can also be stated for correlation-immune functions.

We call an (n, m) function which is t-resilient an (n, m, t)-function. Clearly, if such a function exists, then $m \leq n - t$, since balanced (n, m)-functions can exist only if $m \leq n$. This bound is weak (it is tight if and only if $m = 1$ or $t = 1$). It is shown in [70] (see also [9]) that, if an (n, m, t)-function exists, then $m \leq n - \log_2 \left[\sum_{i=0}^{t/2} \binom{n}{i}\right]$ if t is even and $m \leq n - \log_2 \left[\binom{n-1}{(t-1)/2} + \sum_{i=0}^{(t-1)/2} \binom{n}{i}\right]$ if t is odd. This can be deduced from a classical bound on orthogonal arrays, due to Rao [145]. But, as shown in [9] (see also [127]), potentially better bounds can be deduced from the linear programming bound due to Delsarte [77]: $t \leq \left\lfloor \frac{2^{m-1} n}{2^m - 1} \right\rfloor - 1$ and $t \leq 2 \left\lfloor \frac{2^{m-2}(n+1)}{2^m - 1} \right\rfloor - 1$.

Note that composing a t-resilient (n, m)-function by a permutation on $\mathbb{F}_2^m$ does not change its resiliency order (this obvious result was first observed in [160]). Also, the t-resiliency of S-boxes can be expressed by means of the t-resiliency and t-th order correlation immunity of Boolean functions:

Proposition 32 *Let F be an (n, m) function. Then F is t-resilient if and only if one of the following conditions is satisfied :*
1. for every nonzero vector $v \in \mathbb{F}_2^m$, the Boolean function $v \cdot F(x)$ is t-resilient,
2. for every balanced m-variable Boolean function g, the n-variable Boolean function $g \circ F$ is t-resilient.

Equivalently, F is t-resilient if and only if, for every vector $u \in \mathbb{F}_2^n$ such that $w_H(u) \leq t$, one of the following conditions is satisfied :
(i). $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x} = 0$, for every $v \in \mathbb{F}_2^{m*}$,
(ii). $\sum_{x \in \mathbb{F}_2^n} (-1)^{g(F(x)) + u \cdot x} = 0$, for every balanced m-variable Boolean function g.

Finally, F is t-resilient if and only if, for every vector $b \in \mathbb{F}_2^m$, the Boolean function φ_b is t-th order correlation-immune and has weight 2^{n-m}.

Proof. According to the characterization recalled in the previous chapter, Condition 1 (resp. Condition 2) is equivalent to the fact that Condition (i) (resp. Condition (ii)) is satisfied for every vector $u \in \mathbb{F}_2^n$ such that $w_H(u) \leq t$.

Let us prove now that the t-resiliency of F implies Condition 2, which implies Condition 1, which implies that, for every vector $b \in \mathbb{F}_2^m$, the Boolean function φ_b is t-th order correlation-immune and has weight 2^{n-m}, which implies that F is t-resilient. If F is t-resilient, then, for every balanced m-variable Boolean function g, the function $g \circ F$ is t-resilient, by definition; hence Condition 2 is satisfied; this clearly implies Condition 1, since the function $g(x) = v \cdot x$ is balanced for every nonzero vector v. Relation (4) implies then that, for every non-zero vector $u \in \mathbb{F}_2^n$ such that $w_H(u) \leq t$ and for every $b \in \mathbb{F}_2^m$, we have $\widehat{\varphi_b}(u) = 2^{-m} \sum_{x \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m} (-1)^{v \cdot (F(x)+b)+u \cdot x} = 2^{-m} \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} = 0$. Hence, Condition 1 implies that φ_b is t-th order correlation-immune for every b. Also, according to Proposition 2, Condition 1 implies that F is balanced, *i.e.* φ_b has weight 2^{n-m}, for every b. These two conditions obviously imply, by definition, that F is t-resilient. □

Consequently, the t-resiliency of vectorial functions is invariant under the same transformations as for Boolean functions.

4.1 Constructions

4.1.1 Linear or affine resilient functions

The construction of t-resilient linear functions is easy: Bennett et al. [5] and Chor et al. [70] established the connection between linear resilient functions and linear codes (correlation-immune functions being related to orthogonal arrays, see [40, 39], we could in fact refer to Delsarte [78] for this relationship). There exists a linear (n, m, t)-function if and only if there exists a binary linear $[n, m, t+1]$ code.

Proposition 33 *Let G be a generating matrix for an $[n, m, d]$ binary linear code. We define $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ by the rule $L(x) = x \times G^T$, where G^T is the transpose of G. Then L is an $(n, m, d-1)$-function.*

Indeed, for every nonzero $v \in \mathbb{F}_2^m$, the vector $v \cdot L(x) = v \cdot (x \times G^t)$ has the form $x \cdot u$ where $u = v \times G$ is a nonzero codeword. Hence, u has weight at least d and the linear function $v \cdot L$ is $(d-1)$-resilient, since it has at least d independent terms of degree 1 in its ANF.
The converse of Proposition 33 is clearly also true.
Proposition 33 is still trivially true if L is affine instead of linear, that is $L(x) = x \times G^t + a$, where a is a vector of $\mathbb{F}_2^k$.
Stinson [151] considered the equivalence between resilient functions and what he called large sets of orthogonal arrays. According to Proposition 32, an (n, m)-function is t-resilient if and only if there exists a set of 2^m disjoint binary arrays of dimensions $2^{n-m} \times n$, such that, in any t columns of each array, every one of the 2^t elements of $\mathbb{F}_2^t$ occurs in exaclty 2^{n-m-t}

rows and no two rows are identical.
The construction of (n, m, t)-functions by Proposition 33 can be generalized by considering nonlinear codes of length n (that is subsets of $\mathbb{F}_2^n$) and of size 2^{n-m} whose dual distance $d^\perp$ equals $t+1$ (see [152]). In the case of Proposition 33, C is the dual of the code of generating matrix G. As recalled in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", the *dual distance of a code* C of length n is the smallest nonzero integer i such that the coefficient of the monomial $X^{n-i}Y^i$ in the polynomial $\sum_{x,y\in C}(X+Y)^{n-w_H(x+y)}(X-Y)^{w_H(x+y)}$ is nonzero (when the code is linear, the dual distance is equal to the minimum Hamming distance of the dual code, according to MacWilliams' identity). Equivalently, according to the calculations made in the chapter "Boolean Functions for Cryptography and Error Correcting Codes" for proving the MacWilliams identity and to Proposition 32, the dual distance is the number $d^\perp$ such that the indicator of C is $d^\perp$-th order correlation immune. The nonlinear code needs also to be *systematic* (that is, there must exist a subset I of $\{1, \cdots, n\}$ called an *information set* of C, necessarily of size $n-m$ since the code has size 2^{n-m}, such that every possible tuple occurs in exactly one codeword within the specified coordinates $x_i;\ i \in I$) to allow the construction of an $(n, m, d^\perp - 1)$-function: the image of a vector $x \in \mathbb{F}_2^n$ is the unique vector y of $\mathbb{F}_2^n$ such that $y_i = 0$ for every $i \in I$ and such that $x \in y + C$ (in other words, to calculate y, we first determine the unique codeword c of C which matches with x on the information set and we have $y = x + c$). It is deduced in [152] that, for every $r \geq 3$, a $(2^{r+1}, 2^{r+1} - 2r - 2, 5)$-resilient function exists (the construction is based on the Kerdock code), and that no affine resilient function with such good parameters exists.

4.1.2 Maiorana-MacFarland resilient functions

The idea of designing resilient vectorial functions by generalizing the Maiorana-MacFarland construction is natural. One can find a first reference of such construction in a paper by Nyberg [135], but for generating perfect nonlinear functions. This technique has been used by Kurosawa et al. [119], Johansson and Pasalic [113], Pasalic and Maitra [143] and Gupta and Sarkar [99] to produce functions having high resiliency and high nonlinearity[22].

[22] But, as recalled in Section 3.3, this notion of nonlinearity is not relevant to S-boxes for stream ciphers. The unrestricted nonlinearity of resilient functions and of Maiorana-MacFarland functions has to be further studied.

Definition 16 *The class of* Maiorana-McFarland (n, m)*-functions is the set of those functions* F *which can be written in the form:*

$$F(x,y) = x \times \begin{pmatrix} \varphi_{11}(y) & \cdots & \varphi_{1m}(y) \\ \vdots & \ddots & \vdots \\ \varphi_{r1}(y) & \cdots & \varphi_{rm}(y) \end{pmatrix} + H(y), \ (x,y) \in \mathbb{F}_2^r \times \mathbb{F}_2^s \quad (24)$$

where r *and* s *are two integers satisfying* $r + s = n$*,* H *is any* (s, m)*-function and, for every index* $i \leq r$ *and every index* $j \leq m$*,* φ_{ij} *is a Boolean function on* $\mathbb{F}_2^s$*.*

The concatenation of t-resilient functions being still t-resilient, if the transpose matrix of the matrix involved in Equation (24) is the generator matrix of a linear $[r, m, d]$-code for every vector y ranging over $\mathbb{F}_2^s$, then the (n, m)-function F is $(d - 1)$-resilient.

Any Maiorana-McFarland's (n, m)-function F can be written in the form:

$$F(x,y) = \left(\bigoplus_{i=1}^{r} x_i \varphi_{i1}(y) \oplus h_1(y), \ldots, \bigoplus_{i=1}^{r} x_i \varphi_{im}(y) \oplus h_m(y) \right) \quad (25)$$

where $H = (h_1, ..., h_m)$.

After denoting, for every $i \leq m$, by ϕ_i the (s, r)-function which admits the Boolean functions φ_{1i}, ..., φ_{ri} for coordinate functions, we can rewrite Relation (25) as :

$$F(x,y) = \left(x \cdot \phi_1(y) \oplus h_1(y), \ldots, x \cdot \phi_m(y) \oplus h_m(y) \right). \quad (26)$$

- Resiliency: As a direct consequence of Proposition 33, we have (equivalently to what is written above in terms of codes):

Proposition 34 *Let* n*,* m*,* r *and* s *be three integers such that* $n = r + s$*. Let* F *be a Maiorana-McFarland's* (n, m)*-function defined as in Relation (26) and such that, for every* $y \in \mathbb{F}_2^s$*, the family* $(\phi_i(y))_{i \leq m}$ *is a basis of an* m*-dimensional subspace of* $\mathbb{F}_2^r$ *having* $t + 1$ *for minimum Hamming weight, then* F *is at least* t*-resilient.*

- Nonlinearity: According to the known facts about the Walsh transform of the Boolean Maiorana-MacFarland functions, the nonlinearity $nl(F)$ of any Maiorana-McFarland's (n, m)-function defined as in Relation (26) satisfies

$$nl(F) = 2^{n-1} - 2^{r-1} \max_{(u,u') \in \mathbb{F}_2^r \times \mathbb{F}_2^s, v \in \mathbb{F}_2^{m*}} \left| \sum_{y \in E_{u,v}} (-1)^{v \cdot H(y) + u' \cdot y} \right| \tag{27}$$

where $E_{u,v}$ denotes the set $\{y \in \mathbb{F}_2^s;\ \sum_{i=1}^m v_i \phi_i(y) = u\}$.

The bounds proved in the chapter "Boolean Functions for Cryptography and Error Correcting Codes", for the nonlinearities of Maiorana-McFarland's Boolean functions imply that the nonlinearity $nl(F)$ of a Maiorana-McFarland's (n, m)-function defined as in Relation (26) satisfies

$$2^{n-1} - 2^{r-1} \max_{u \in \mathbb{F}_2^r, v \in \mathbb{F}_2^{m*}} |E_{u,v}| \leq nl(F) \leq 2^{n-1} - 2^{r-1} \left\lceil \sqrt{\max_{u \in \mathbb{F}_2^r, v \in \mathbb{F}_2^{m*}} |E_{u,v}|} \right\rceil.$$

If, for every element y, the vectorspace spanned by the vectors $\phi_1(y)$, ..., $\phi_m(y)$ admits m for dimension and has a minimum Hamming weight strictly greater than k (so that F is t-resilient with $t \geq k$), then we have

$$nl(F) \leq 2^{n-1} - 2^{r-1} \left\lceil \frac{2^{s/2}}{\sqrt{\sum_{i=k+1}^r \binom{r}{i}}} \right\rceil. \tag{28}$$

The nonlinearity can be exactly calculated in two situations (at least): if, for every vector $v \in \mathbb{F}_2^{m*}$, the (s, r)-function $y \mapsto \sum_{i \leq m} v_i \phi_i(y)$ is injective, then F admits $2^{n-1} - 2^{r-1}$ for nonlinearity; and if, for every vector $v \in \mathbb{F}_2^{m*}$, this same function takes exactly two times each value of its image set, then F admits $2^{n-1} - 2^r$ for nonlinearity.

Johansson and Pasalic described in [113] a way to specify the vectorial functions ϕ_1, ..., ϕ_m so that this kind of condition is satisfied. Their result can be generalized in the following form:

Lemma 1 *Let C be a binary linear $[r, m, t+1]$ code. Let $\beta_1, \ldots, \beta_m$ be a basis of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_{2^m}$, and let L_0 be a linear isomorphism between $\mathbb{F}_{2^m}$ and C. Then the functions $L_i(z) = L_0(\beta_i z)$, $i = 1, \ldots, m$, have the property that, for every vector $v \in \mathbb{F}_2^{m*}$, the function $z \in \mathbb{F}_{2^m} \mapsto \sum_{i=1}^m v_i L_i(z)$ is a bijection from $\mathbb{F}_{2^m}$ into C.*

Proof. For every vector v in $\mathbb{F}_2^m$ and every element z of $\mathbb{F}_{2^m}$, we have $\sum_{i=1}^m v_i L_i(z) = L_0\left((\sum_{i=1}^m v_i \beta_i) z\right)$. If the vector v is nonzero, then the element $\sum_{i=1}^m v_i \beta_i$ is nonzero. Hence, the function $z \in \mathbb{F}_{2^m} \mapsto \sum_{i=1}^m v_i L_i(z)$ is a bijection. □

Since the functions $L_1, L_2, \cdots, L_m$ vanish at $(0,\ldots,0)$, they do not satisfy the hypothesis of Proposition 34 (i.e. the vectors $L_1(z)$, ..., $L_m(z)$ are not linearly independent for every $z \in \mathbb{F}_{2^m}$). A solution to derive a family of vectorial functions also satisfying the hypothesis of Proposition 34 is then to right-compose the functions L_i with a same injective (or two-to-one) function π from $\mathbb{F}_2^s$ into $\mathbb{F}_{2^m}^*$. Then, for every nonzero vector $v \in \mathbb{F}_2^{m*}$, the function $y \in \mathbb{F}_2^s \mapsto \sum_{i=1}^m v_i L_i[\pi(y)]$ is injective from $\mathbb{F}_2^s$ into C^*.
This gives the following construction[23]:
Given two integers m and r ($m < r$), construct an $[r, m, t+1]$-code C such that t is as large as possible (Brouwer gives in [22] a precise overview of the best known parameters of codes). Then, define m linear functions L_1, ..., L_m from $\mathbb{F}_{2^m}$ into C as in Lemma 1. Choose an integer s strictly lower than m (resp. lower than or equal to m) and define an injective (resp. two-to-one) function π from $\mathbb{F}_2^s$ into $\mathbb{F}_{2^m}^*$. Choose any (s, m)-function $H = (h_1, \ldots, h_m)$ and denote $r + s$ by n. Then the (n, m)-function F whose coordinate functions are defined by $f_i(x, y) = x \cdot [L_i \circ \pi](y) \oplus h_i(y)$ is t-resilient and admits $2^{n-1} - 2^{r-1}$ (resp. $2^{n-1} - 2^r$) for nonlinearity.
All the primary constructions presented in [113, 119, 143, 136] are based on this principle. Also, the recent construction of (n, m, t)-functions defined by Gupta and Sarkar in [99] is also a particular application of this construction, as shown in [63].

4.1.3 Other constructions

Constructions of highly nonlinear resilient vectorial functions, based on elliptic curves theory and on the trace of some power functions $x \mapsto x^d$ on finite fields, have been designed respectively by Cheon [68] and by Khoo and Gong [117]. However, it is still an open problem to design highly nonlinear functions with high algebraic degrees and high resiliency orders with Cheon's method. Besides, the number of functions which can be designed by these methods is very small.
Zhang and Zheng proposed in [160, 161] a secondary construction consisting in the composition $F = G \circ L$ of a linear resilient (n, m, t)-function L

[23] Another construction based on Lemma 1 is given by Johansson and Pasalic in the same paper [113]. It involves a family of *nonintersecting codes*, that is a family of codes having the same parameters (same length, same dimension and same minimum distance) and whose pairwise intersections are reduced to the null vector. However, this construction is often worse for large resiliency orders, as shown in [63].

with a highly nonlinear (m, k)-function. F is obviously t-resilient, admits $2^{n-m} nl(G)$ for nonlinearity where $nl(G)$ denotes the nonlinearity of G and its degree is the same as that of G. Taking for function G the inverse function $x \mapsto x^{-1}$ on the finite Field $\mathbb{F}_{2^m}$ studied by Nyberg in [137] (and later used for designing the S-boxes of the AES), Zhang and Zheng obtained t-resilient functions having a nonlinearity larger than or equal to $2^{n-1} - 2^{n-m/2}$ and having $m-1$ for algebraic degree. But the linear (n, m)-functions involved in the construction of Zhang and Zheng introduce a weakness: their *unrestricted nonlinearity* being null, this kind of functions can not be used as a multi-output combination function in stream ciphers. Nevertheless, this drawback can be avoided by concatenating such functions (recall that the concatenation of t-resilient functions gives t-resilient functions, and a good nonlinearity can be obtained by concatenating functions with disjoint Walsh supports). We obtain this way a modified Maiorana-McFarland's construction, which should be investigated.

Other secondary constructions of resilient vectorial functions can be derived from the secondary constructions of resilient Boolean functions. (see *e.g.* [39, 51]).

Acknowledgement

We thank Lilya Budaghyan, Anne Canteaut and Gregor Leander for useful comments and Caroline Fontaine for her careful reading of a previous draft of this chapter.

References

[1] F. Armknecht and M. Krause. Constructing single- and multi-output boolean functions with maximal immunity. *Proceedings of ICALP 2006, Lecture Notes of Computer Science* 4052, pp. 180-191, 2006.

[2] G. Ars and J.-C. Faugère. Algebraic immunities of functions over finite fields. *Proceedings of the conference BFCA 2005*, pp. 21-38, 2005.

[3] L.A. Bassalygo, G.V. Zaitsev and V.A. Zinoviev, Uniformly packed codes. *Problems of Information Transmission*, vol. 10, No 1, pp. 9-14, 1974.

[4] L.A. Bassalygo and V.A. Zinoviev. Remarks on uniformly packed codes. *Problems of Information Transmission*, vol. 13, No 3, pp. 22-25, 1977.

[5] C. H. Bennett, G. Brassard and J. M. Robert. Privacy amplification by public discassion. *SIAM J. Computing 17*, pp. 210-229, 1988.

[6] T. Bending and D. Fon-Der-Flaass. Crooked functions, bent functions and distance regular graphs. *Electron. J. Comb.*, Vol. 5, Research paper 34 (electronic), 14 pages, 1998.

[7] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4160-4170, 2006.

[8] T. Beth and C. Ding, On almost perfect nonlinear permutations. *Proceedings of Eurocrypt' 93, Lecture Notes in Computer Science* 765, pp. 65-76, 1994.

[9] J. Bierbrauer, K. Gopalakrishnan and D.R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds. *SIAM J. Discrete Math.*, Vol. 9, no. 3, pp. 424-452, 1996.

[10] J. Bierbrauer and G. Kyureghyan. Crooked binomials. *Designs Codes Cryptography* 46(3), pp. 269-301, 2008.

[11] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, Vol 4, no.1, pp. 3-72, 1991.

[12] A. Biryukov and D. Wagner. Slide Attacks. *Proceedings of the 6th International Workshop on Fast Software Encryption, Lecture Notes in Computer Science* 1636, pp.245259, 1999.

[13] C. Bracken, E. Byrne, N. Markin and G. McGuire. On the Walsh Spectrum of a New APN Function. *Proceedings of IMA conference on Cryptography and Coding, Lecture Notes in Computer Science* 4887, pp. 92-98, 2007.

[14] C. Bracken, E. Byrne, N. Markin and G. McGuire. Determining the Nonlinearity of a New Family of APN Functions. *Proceedings of AAECC-17 Conference, Lecture Notes in Computer Science* 4851, pp. 72-79, 2007.

[15] C. Bracken, E. Byrne, N. Markin and G. McGuire. An infinite family of quadratic quadrinomial APN functions. arXiv:0707.1223v1, 2007.

[16] C. Bracken, E. Byrne, N. Markin and G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and their Applications* 14, pp. 703-714, 2008.

[17] C. Bracken, E. Byrne, N. Markin and G. McGuire. A few more quadratic APN functions. arXiv:0804.4799v1, 2007.

[18] C. Bracken, E. Byrne, G. McGuire and G. Nebe. On the equivalence of quadratic APN functions. To appear in *Designs, Codes and Cryptography*, 2011.

[19] C. Bracken and G. Leander. New families of functions with differential uniformity of 4. Proceedings of the conference BFCA 2008, Copenhagen, to appear.

[20] C. Bracken and G. Leander. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. *Finite Fields and Their Applications* 16(4), pp. 231-242, 2010.

[21] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, Volume 49 , Issue 1-3, pp. 273-288, 2008. Revised and extended version of a paper with the same title in the Proceedings of the Workshop on Coding and Cryptography WCC 2007, pp. 39-48, 2007

[22] A.E. Brouwer, Bounds on the minimum distance of linear codes (Table of the best known codes). URL: http://www.win.tue.nl/ aeb/voorlincod.html.

[23] K. Browning, J. F. Dillon, R. E. Kibler and M. McQuistan. APN polynomials and related codes. Special volume of Journal of Combinatorics, Information and System Sciences, honoring the 75-th birthday of Prof. D.K.Ray-Chaudhuri, vol. 34, Issue 1-4, pp. 135-159, 2009.

[24] L. Budaghyan. PhD thesis. The Equivalence of Almost Bent and Almost Perfect Nonlinear Functions and Their Generalizations. Otto-von-Guericke-University, 2005.

[25] L. Budaghyan. The simplest method for constructing APN polynomials EA-inequivalent to power functions. *Proceedings of the International Workshop on the Arithmetic of Finite Fields, WAIFI 2007, Lecture Notes in Computer Science* 4547, pp. 177-188, 2007.

[26] L. Budaghyan, C. Carlet and A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials. *Proceedings of the Workshop on Coding and Cryptography 2005*, Bergen, pp. 306-315, 2005.

[27] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006. This is a completed version of [26].

[28] L. Budaghyan, C. Carlet, P. Felke and G. Leander. An infinite class of quadratic APN functions which are not equivalent to power functions. *Proceedings of IEEE International Symposium on Information Theory (ISIT) 2006.*

[29] L. Budaghyan, C. Carlet and G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Trans. Inform. Theory* vol. 54, no. 9, pp. 4218-4229, 2008. This paper is a completed and merged version of [28] and [31].

[30] L. Budaghyan, C. Carlet and G. Leander. On inequivalence between known power APN functions. Proceedings of the conference BFCA 2008, Copenhagen, to appear.

[31] L. Budaghyan, C. Carlet and G. Leander. Another class of quadratic APN binomials over $\mathbb{F}_{2^n}$: the case n divisible by 4. *Proceedings of the Workshop on Coding and Cryptography, WCC 2007*, pp. 49-58, 2007.

[32] L. Budaghyan, C. Carlet and G. Leander. Constructing new APN functions from known ones. To appear in Finite Fields and Applications, 2008.

[33] L. Budaghyan and C. Carlet. Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. *IEEE Trans. Inform. Theory*, vol. 54, no. 5, pp. 2354-2357, 2008.

[34] L. Budaghyan and A. Pott. On Differential Uniformity and Nonlinearity of Functions. To appear in the Special Issue of Discrete Mathematics devoted to "Combinatorics 2006".

[35] E. Byrne and G. McGuire. On the non-existence of crooked functions on finite fields. *Proceedings of the Workshop on Coding and Cryptography, WCC 2005*, pp. 316-324, 2005.

[36] A.R. Calderbank, G. McGuire, B. Poonen and M. Rubinstein, *On a conjecture of Helleseth regarding pairs of binary m-sequences*, IEEE Transactions on Information Theory, vol 42, pp. 988-990 (1996).

[37] P. Camion and A. Canteaut. Construction of t-resilient functions over a finite alphabet, *Proceedings of EUROCRYPT'96, Lecture Notes in Computer Sciences* 1070, pp. 283-293, 1996.

[38] P. Camion and A. Canteaut. Generalization of Siegenthaler inequality and Schnorr-Vaudenay multipermutations. *Proceedings of CRYPTO'96, Lecture Notes in Computer Science* 1109, pp. 372–386, 1996.

[39] P. Camion and A. Canteaut. Correlation-immune and resilient functions over finite alphabets and their applications in cryptography. *Designs, Codes and Cryptography* 16, pp. 121-149, 1999.

[40] P. Camion, C. Carlet, P. Charpin, N. Sendrier. On correlation-immune functions, *Proceedings of CRYPTO'91, Lecture Notes in Computer Science* 576, pp. 86-100, 1991.

[41] A. Canteaut. Differential cryptanalysis of Feistel ciphers and differentially uniform mappings . *Proceedings of Selected Areas on Cryptography, SAC'97*, pp. 172-184, Ottawa, Canada, 1997.

[42] A. Canteaut. Cryptographic functions and design criteria for block ciphers. *Proceedings of INDOCRYPT 2001, Lecture Notes in Computer Science* 2247, pp. 1-16, 2001.

[43] A. Canteaut. Analysis and design of symmetric ciphers. Habilitation for directing Theses, University of Paris 6, 2006.

[44] A. Canteaut, P. Charpin, and H. Dobbertin. A new characterization of almost bent functions. *Proceedings of Fast Software Encryption 99, Lecture Notes in Computer Science* 1636, pp. 186-200, 1999.

[45] A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 4-8, 2000.

[46] A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1), pp. 105–138, 2000.

[47] A. Canteaut, P. Charpin, and M. Videau. Cryptanalysis of block ciphers and weight divisibility of some binary codes. *Information, Coding and*

Mathematics (Workshop in honor of Bob McEliece's 60th birthday). Kluwer, pp. 75-97, 2002.

[48] A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. *Proceedings of EUROCRYPT 2002, Lecture Notes in Computer Science* 2332, pp. 518-533, 2002.

[49] C. Carlet. A construction of bent functions. *Finite Fields and Applications, London Mathematical Society*, Lecture Series 233, Cambridge University Press, pp. 47-58, 1996.

[50] C. Carlet. On the confusion and diffusion properties of Maiorana-McFarland's and extended Maiorana-McFarland's functions. *Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity* 20, pp. 182-204, 2004.

[51] C. Carlet. On the secondary constructions of resilient and bent functions. *Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, Birkhäuser Verlag*, pp. 3-28, 2004.

[52] C. Carlet. Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications. *IEEE Transactions on Information Theory*, vol.54, no. 3, pp. 1262-1272, 2008.

[53] C. Carlet. On the higher order nonlinearities of Boolean functions and S-boxes, and their generalizations. *Proceedings of SETA 2008, Lecture Notes in Computer Science* 5203, pp. 345-367, 2008.

[54] C. Carlet. On almost perfect nonlinear functions. *Special Section on Signal Design and its Application in Communications, IEICE Trans. Fundamentals*, Vol. E91-A, no. 12, pp. 3665-3678, 2008.

[55] C. Carlet. On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions. *NATO Science for Peace and Security Series, D: Information and Communication Security - Vol 23; Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, pp. 104-116, 2009.

[56] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

[57] C. Carlet and C. Ding. Highly Nonlinear Mappings. *Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity* 20, pp. 205-244, 2004.

[58] C. Carlet and C. Ding. Nonlinearities of S-boxes. *Finite Fields and its Applications* Vol. 13 Issue 1, pp. 121-135, January 2007.

[59] C. Carlet, K. Khoo, C.-W. Lim and C.-W. Loe. Generalized correlation analysis of vectorial Boolean functions. *Proceedings of FSE 2007. Lecture Notes in Computer Science* 4593, pp. 382-398, 2007.

[60] C. Carlet, K. Khoo, C.-W. Lim and C.-W. Loe. On an improved correlation analysis of stream ciphers using multi-output Boolean functions and the related generalized notion of nonlinearity. *Advances in Mathematics of Communications*, Vol. 2, no. 2, pp. 201-221, 2008.

[61] C. Carlet and S. Mesnager. On the construction of bent vectorial functions. Special Issue of *International Journal of Information and Coding Theory* (IJICoT), Vol. 1, no 2, dedicated to Vera Pless, pp. 133-148, 2010.

[62] C. Carlet and E. Prouff. On a new notion of nonlinearity relevant to multi-output pseudo-random generators. *Proceedings of Selected Areas in Cryptography 2003, Lecture Notes in Computer Science* 3006, pp. 291–305, 2004.

[63] C. Carlet and E. Prouff. Vectorial Functions and Covering Sequences. *Proceedings of Finite Fields and Applications, Fq7, Lecture Notes in Computer Science* 2948, pp. 215-248, 2004.

[64] L. Carlitz and S. Uchiyama. Bounds for exponential sums. *Duke Math. Journal* 1, pp. 37-41, 1957.

[65] F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science* 950, pp. 356-365, 1995.

[66] S. Chanson, C. Ding and A. Salomaa. Cartesian authentication codes from functions with optimal nonlinearity. *Theoretical Computer Science* 290, pp. 1737-1752, 2003.

[67] P. Charpin and E. Pasalic. Highly nonlinear resilient functions through disjoint codes in projecting spaces. *Designs, Codes and Cryptography*, 37, pp. 319-346, 2005.

[68] J. H. Cheon. Nonlinear vector resilient functions. *Proceedings of CRYPTO 2001, Lecture Notes in Computer Science* 2139, pp. 458-469, 2001.

[69] J. H. Cheon and D. H. Lee. Resistance of S-Boxes against Algebraic Attacks. *Proceedings of FSE 2004, Lecture Notes in Computer Science* 3017, pp. 83-94, 2004.

[70] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky. The bit extraction problem or t-resilient functions. *Proceedings of the 26th IEEE Symp. on Foundations of Computer Science*, pp. 396-407, 1985.

[71] S. D. Cohen and R. W. Matthews. A class of exceptional polynomials. *Transactions of the AMS* 345, pp. 897-909, 1994.

[72] N. Courtois, B. Debraize and E. Garrido. On exact algebraic [non-]immunity of S-boxes based on power functions. IACR e-print archive 2005/203.

[73] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. *Proceedings of ASIACRYPT 2002, Lecture Notes in Computer Science* 2501, pp. 267-287, 2003.

[74] T. W. Cusick and H. Dobbertin, Some new 3-valued crosscorrelation functions of binary sequences, *IEEE Trans. Inform. Theory*, vol. 42, pp. 1238-1240, 1996.

[75] J. Daemen and V. Rijmen. AES proposal: Rijndael, 1999. See http://www.daimi.au.dk/ ivan/rijndael.pdf See also http://www.quadibloc.com/crypto/co040401.htm

[76] E. R. van Dam and D. Fon-Der-Flaass. Codes, graphs, and schemes from nonlinear functions. *Eur. J. Comb.* 24(1), pp. 85-98, 2003.

[77] P. Delsarte. Bounds for unrestricted codes, by linear programming. *Philips Research Reports* 27, pp. 272-289, 1972.

[78] P. Delsarte. An algebraic approach to the association schemes of coding theory. PhD thesis. Université Catholique de Louvain, 1973.

[79] J. F. Dillon. APN polynomials and related codes. Banff Conference, November 2006.

[80] K. Browning, J. F. Dillon, M. McQuistan and A.J. Wolfe. An APN permutation in dimension 6. Proceedings of *Conference Finite Fields and Applications Fq9*, Contemporary Mathematics 518, pp. 33-42, 2009.

[81] J. F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes and Cryptography* 17, pp. 225-235, 1999.

[82] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Applications* 10, pp. 342-389, 2004.

[83] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. *Proceedings of Fast Software Encryption, Second International Workshop, Lecture Notes in Computer Science* 1008, pp. 61-74, 1995.

[84] H. Dobbertin. One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. *Appl. Algebra Eng. Commun. Comput.* 9 (2), pp. 139-152, 1998.

[85] H. Dobbertin. Kasami power functions, permutation polynomials and cyclic difference sets. *Proceedings of the NATO-A.S.I. Workshop "Difference sets, sequences and their correlation properties"*, Bad Windsheim, Kluwer Verlag, pp. 133-158, 1998.

[86] H. Dobbertin. Another proof of Kasami's Theorem. *Designs, Codes and Cryptography* 17, pp. 177-180, 1999.

[87] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case, *IEEE Trans. Inform. Theory*, vol. 45, no. 4, pp. 1271-1275, 1999.

[88] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Niho case, *Information and Computation* 151, pp. 57-72, 1999.

[89] H. Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: a new case for n divisible by 5. *Proceedings of Finite Fields and Applications* Fq5, Augsburg, Germany, Springer, pp. 113-121, 2000.

[90] H. Dobbertin. Uniformly representable permutation polynomials. *Proceedings of Sequences and their Applications, SETA 01, Discrete Mathematics and Theoretical Computer Science*, Springer, pp. 1-22, 2002.

[91] H. Dobbertin. Private communication, 1998.

[92] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit. Construction of Bent Functions via Niho Power Functions. *Journal of Combinatorial Theory, Series A*, Volume 113, Issue 5, pp. 779-798, 2006.

[93] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory* vol. 52, no. 2, pp. 744-747, 2006.

[94] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, vol. 3, no. 1, pp. 59-81, 2009.

[95] K. Feng, Q. Liao and J. Yang. Maximal values of generalized algebraic immunity. To appear in Designs, Codes and Cryptography.

[96] J. Friedman. The bit extraction problem. *Proceedings of the 33th IEEE Symp. on Foundations of Computer Science*, pp. 314-319, 1992.

[97] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory*, vol. 14, pp. 154-156, 1968.

[98] F. Göloglu and A. Pott. Results on the crosscorrelation and autocorrelation of sequences. *Proceedings of Sequences and their Applications - SETA 2008 - Lecture Notes in Computer Science* 5203, pp. 95-105, 2008.

[99] K. Gupta and P. Sarkar. Improved Construction of Nonlinear Resilient S-Boxes. *Proceedings of ASIACRYPT 2002, Lecture Notes in Computer Science* 2501, pp. 466-483, 2002.

[100] K. Gupta and P. Sarkar. Construction of perfect nonlinear and maximally nonlinear multiple-output Boolean functions satisfying higher order strict avalanche criteria. *IEEE Transactions on Inform. Theory*, vol. 50, pp. 2886-2894, 2004.

[101] T. Helleseth and P. V. Kumar. Sequences with low correlation. In *Handbook of Coding Theory*, V. Pless and W.C. Huffman Eds. Amsterdam, The Netherlands: Elsevier, vol. II, pp. 1765-1854, 1998.

[102] T. Helleseth and D. Sandberg. Some power mappings with low differential uniformity. *Applic. Alg. Eng., Commun. Comput.*, vol. 8, pp. 363-370, 1997.

[103] T. Helleseth, C. Rong and D. Sandberg. New families of almost perfect nonlinear power mappings. *IEEE Transactions on Inform. Theory*, vol. 45, pp. 475-485, 1999.

[104] T. Helleseth and V. Zinoviev. On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums. *Designs, Codes and Cryptography* 17, pp. 269-288, 1999.

[105] D. Hertel, A. Pott, Two results on maximum nonlinear functions, Des. Codes Crypt., in press, 2009.

[106] H. Hollman and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fileds and Their Applications* 7, pp. 253-286, 2001.

[107] K. Horadam. *Hadamard Matrices and their Applications.* Princeton University Press, 2006.

[108] X.-d. Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Proceedings of the Workshop on Coding and Cryptography* WCC 2003, pp. 273-280, 2003. Completed version in *Discrete Applied Mathematics* 154, Issue 2, pp. 313-325, 2006.

[109] T. Iwata and K. Kurosawa. Probabilistic higher order differential attack and higher order bent functions. *Proceedings of ASIACRYPT 1999, Lecture Notes in Computer Science* 1716, pp. 62-74, 1999.

[110] T. Jakobsen and L.R. Knudsen. The interpolation attack on block ciphers. *Proceedings of Fast Software Encryption'97, Lecture Notes in Computer Science* 1267, pp. 28-40, 1997.

[111] H. Janwa and R. Wilson, Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. *Proceedings of AAECC-10, Lecture Notes in Computer Science* 673, pp. 180–194, 1993.

[112] D. Jedlicka. APN monomials over $GF(2^n)$ for infinitely many n. Preprint.

[113] T. Johansson and E. Pasalic. A construction of resilient functions with high nonlinearity. *Proceedings of the IEEE International Symposium on Information Theory* Sorrente, Italy, 2000.

[114] D. Jungnickel and A. Pott. Difference sets: An introduction. In *Difference sets, Sequences and their Autocorrelation Properties*, A. Pott, P.V. Kumar, T. Helleseth and D. Jungnickel, Eds. Amsterdam, The Netherlands: Kluwer, pp. 259-295, 1999.

[115] T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Information and Control* 18, pp. 369-394, 1971.

[116] K. Khoo, G. Gong and D. Stinson. Highly nonlinear S-boxes with reduced bound on maximum correlation. *Proceedings of 2003 IEEE International Symposium on Information Theory*, 2003. http://www.cacr.math.uwaterloo.ca/techreports/2003/corr2003-12.ps

[117] K. Khoo and G. Gong. New constructions for resilient and highly nonlinear Boolean functions. *Proceedings of 8th Australasian Conference, ACISP 2003, Lecture Notes in Computer Science* 2727, pp. 498-509, 2003.

[118] L. Knudsen. Truncated and higher order differentials. *Proceedings of Fast Software Encryption, Second International Workshop, Lecture Notes in Computer Science* 1008, pp. 196-211, 1995.

[119] K. Kurosawa, T. Satoh and K. Yamamoto. Highly Nonlinear t-Resilient Functions. *Journal of Universal Computer Science* vol. 3, no 6, pp. 721–729, 1997.

[120] G. Kyureghyan. Differentially affine maps. *Proceedings of the Workshop on Coding and Cryptography, WCC 2005*, pp. 296-305, 2005.

[121] G. Kyureghyan. The only crooked power functions are $x^{2^k+2^l}$. *Eur. J. Comb.* 28(4), pp. 1345-1350, 2007.

[122] G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.

[123] J. Lahtonen, G. McGuire and H. Ward. Gold and Kasami-Welch functions, quadratic forms and bent functions. *Advances of Mathematics of Communication*, vol. 1, pp. 243-250, 2007.

[124] X. Lai. Higher order derivatives and differential cryptanalysis. *Proceedings of the "Symposium on Communication, Coding and Cryptog-*

raphy", in honor of J. L. Massey on the occasion of his 60'th birthday. 1994.

[125] P. Langevin and P. Véron. On the nonlinearity of power functions. *Designs, Codes and Cryptography* 37, pp. 31 - 43, 2005.

[126] G. Leander and P. Langevin. On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin. *Proceedings of "The first Symposium on Algebraic Geometry and its Applications" (SAGA'07), Tahiti, 2007, published by World Scientific, Series on Number Theory and its Applications*, Vol. 5, pp. 410-418, 2008.

[127] V. I. Levenshtein. Split Orthogonal Arrays and Maximum Independent Resilient Systems of Functions. *Des. Codes Cryptography* 12(2), pp. 131-160, 1997.

[128] Q. Liao and K. Feng. A note on algebraic immunity of vectorial Boolean functions. Preprint.

[129] R. Lidl and H. Niederreiter. *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachussetts, 1983.

[130] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, Amsterdam, North Holland. 1977.

[131] M. Matsui. Linear cryptanalysis method for DES cipher. *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science* 765, pp. 386-397, 1994.

[132] G. McGuire and A.R. Calderbank. Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences. *IEEE transactions on information theory*, vol. 41, no. 4, pp. 1153-1155, 1995.

[133] N. Nakagawa and S. Yoshiara. A construction of differentially 4-uniform functions from commutative semifields of characteristic 2. *Proceedings of the International Workshop on the Arithmetic of Finite Fields, WAIFI 2007, Lecture Notes in Computer Science* 4547, pp. 134-146, 2007.

[134] Y.Nawaz, K.Gupta and G.Gong. Efficient Techniques to find algebraic immunity of S-boxes based on power mappings. *Proceedings of the Workshop on Coding and Cryptography 2007* WCC, pp. 237-246, 2007.

[135] K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.

[136] K. Nyberg. On the construction of highly nonlinear permutations. *Proceedings of EUROCRYPT' 92, Lecture Notes in Computer Science* 658, pp. 92-98, 1993.

[137] K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.

[138] K. Nyberg. New bent mappings suitable for fast implementation. *Proceedings of Fast Software Encryption 1993, Lecture Notes in Computer Science* 809, pp. 179-184, 1994.

[139] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption 1994, Lecture Notes in Computer Science* 1008, pp. 111-130, 1995.

[140] K. Nyberg. Correlation theorems in crytptanalysis. *Discrete Applied Mathematics* 111 (Special Issue on Coding and Cryptography), pp. 177-188, 2000.

[141] K. Nyberg. Multidimensional Walsh transform and a characterization of bent functions. *Proceedings of Information Theory Workshop ITW 2007*, Bergen, Norway, July 2007.

[142] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. *Proceedings of CRYPT0' 92, Lecture Notes in Computer Science* 740, pp. 566-574, 1993.

[143] E. Pasalic and S. Maitra. Linear Codes in Generalized Construction of Resilient Functions with Very High Nonlinearity. *IEEE Transactions on Information Theory*, vol. 48, pp. 2182- 2191, 2002, completed version of a paper published in the *Proceedings of Selected Areas in Cryptography, SAC 2001, Lecture Notes in Computer Science* 2259, pp. 60-74, 2002.

[144] E. Prouff. DPA attacks and S-boxes. *Proceedings of Fast Software Encryption 2005, Lecture Notes in Computer Science* 3557, pp. 424-442, 2005.

[145] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *J. Royal Statist. Soc.* 9, pp. 128-139, 1947.

[146] F. Rodier Bounds on the degrees of APN polynomials. Proceedings of the conference BFCA 2008, Copenhagen, to appear.

[147] T. Satoh, T. Iwata and K. Kurosawa. On cryptographically secure vectorial Boolean functions. *Proceedings of Asiacrypt 1999, Lecture Notes in Computer Science* 1716, pp. 20-28, 1999.

[148] J. Seberry, X.-M. Zhang and Y. Zheng. Nonlinearity characteristics of quadratic substitution boxes. *Proceedings of Selected Areas in Cryptography (SAC'94)*. This paper appeared under the title "Relationship among Nonlinearity Criteria" in the *Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science*, 950 pp. 376-388, 1995.

[149] T. Shimoyama and T. Kaneko. Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES. *Proceedings of CRYPTO 98, Lecture Notes In Computer Science* 1462, pp. 200-211, 1998.

[150] V. M. Sidelnikov. *On the mutual correlation of sequences*, Soviet Math. Dokl. 12, pp. 197-201, 1971.

[151] D.R. Stinson. Resilient functions and large sets of orthogonal arrays. *Congressus Numer.*, vol 92, pp. 105-110, 1993.

[152] D.R. Stinson and J.L. Massey. An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. *Journal of Cryptology*, vol 8, n° 3, pp. 167-173, 1995.

[153] A. Tardy-Corfdir and H. Gilbert. A known plaintext attack on feal-4 and feal-6. In *Proceedings of CRYPTO'91, Lecture Notes in Computer Science* 576, pp. 172-181, 1991.

[154] S. Vaudenay. On the need for multipermutations: cryptanalysis of MD4 and SAFER. *Proceedings of Fast Software Encryption, Lecture Notes in Computer Science* 1008, pp. 286-297, 1995.

[155] J. F. Voloch. Symmetric cryptography and algebraic curves. *Proceedings of "The first Symposium on Algebraic Geometry and its Applications" (SAGA'07), Tahiti, 2007, published by World Scientific, Series on Number Theory and its Applications*, Vol. 5, pp. 135-141, 2008.

[156] T. Wadayama, T. Hada, K. Wagasugi and M. Kasahara. Upper and lower bounds on the maximum nonlinearity of n-input m-output

Boolean functions. *Designs, Codes and Cryptography* 23, pp. 23–33, 2001.

[157] A.F. Webster and S.E. Tavares. On the design of S-boxes. In *Proceedings of CRYPTO'85, Lecture Notes in Computer Science* 219, pp. 523–534, 1985.

[158] I. Wegener, *The complexity of Boolean functions*, Stuttgart, B. G. Teubner, Chichester, John Wiley & Sons, 1987.

[159] L. Welch, Lower bounds on the maximum cross correlation of signals. *IEEE Trans. Inform. Theory* vol. 20, no. 3, pp. 397-399, 1974.

[160] X.-M. Zhang and Y. Zheng. On Nonlinear Resilient Functions. *Proceedings of EUROCRYPT '95, Lecture Notes in Computer Science* 921, pp. 274-288, 1995.

[161] X.-M. Zhang and Y. Zheng. Cryptographically Resilient Functions. *IEEE Transactions on Information Theory*, vol. 43, pp. 1740-1747, 1997.

[162] M. Zhang and A. Chan. Maximum correlation analysis of nonlinear S-boxes in stream ciphers. *Proceedings of CRYPTO 2000, Lecture Notes in Computer Science* 1880, pp. 501-514, 2000.

[163] Y. Zhou and C. Li. The Walsh spectrum of a new family of APN functions. *Proceedings of WSPC*, 2008.

Index