

Bent functions: fundamentals and results

Sihem Mesnager

Overview	1
1 Generalities on Boolean functions and p-ary functions	5
1.1 Boolean functions	5
1.1.1 Background on Boolean functions	5
1.1.2 Boolean functions: representations	7
Algebraic normal Form	7
Numerical normal form	7
Trace function and the polynomial form	9
The bivariate representation	11
From a representation to another	12
1.1.3 Boolean functions of low degree	14
1.2 An equivalent notion on Boolean functions	14
1.3 On p -ary functions	14
1.3.1 Trace functions	14
1.3.2 p -ary functions-representations	15
1.3.3 Quadratic form over finite fields in characteristic p	16
2 Mathematical foundations	19
2.1 Special polynomials over finite fields	20
2.1.1 Permutations polynomials	20
2.1.2 Polynomials e -to-1	20
2.1.3 Involutions	20
2.1.4 Binary Dickson polynomial	21
2.2 Fourier transform and Walsh Hadamard transform	24
2.3 Some classical binary exponential sums	27
2.3.1 Binary Kloosterman sums	27
2.3.2 Binary cubic sums	28
2.3.3 Partial exponential sums	28
2.4 Some results on the sum over the cyclic group U of characters	29
2.5 Some basic notions in number theory	37
2.5.1 Quadratic Residues	38
2.5.2 Group characters and Gauss sums	39
2.6 Cyclotomic field $\mathbb{Q}(\xi_p)$	40
3 Boolean functions and cryptography	43
3.1 Cryptographic framework for Boolean functions	43
3.2 Main cryptographic criteria for Boolean functions	45
3.2.1 Algebraic degree	45
3.2.2 Balancedness	45
3.2.3 Nonlinearity	45
3.2.4 Correlation immune and resiliency	46
3.2.5 Algebraic immunity	46
3.3 Trade-offs between the different criteria	47
3.4 Recent constructions of Boolean functions satisfying the main cryptographic criteria	48
3.5 Some results on a conjecture about binary strings distribution	54

4	Bent functions-generalities	65
4.1	Bent functions: introduction-historical notes	65
4.2	Bent Boolean functions: definition and properties	66
4.3	Equivalent characterizations of bent Boolean functions	68
4.4	Enumeration of bent functions and bounds	72
4.4.1	An overview on the state of the art	72
4.4.2	A conjecture related to the number of bent functions	73
4.5	Classification and equivalence	73
4.6	Geometric properties of bent functions and their representation over the integers	74
4.7	Decompositions of bent functions	75
4.8	Bent functions and normality	75
4.9	Bent functions: applications	77
4.9.1	Bent functions in coding theory	77
4.9.2	Bent functions in cryptography	79
	Weakness of the cryptographic bent functions	79
4.9.3	Bent functions and their connections to combinatorics	80
5	Bent functions: primary constructions (part I)	87
5.1	Two main general classes of bent functions	87
5.1.1	Maiorana-McFarland's class	88
5.1.2	The Partial Spread class \mathcal{PS}	88
5.2	Basic primary constructions of bent functions in multivariate representation . . .	90
5.3	Primary constructions of bent functions in bivariate representation	90
5.4	Primary constructions and characterization of bent functions in polynomial form	91
5.4.1	Monomial bent functions	91
5.4.2	Binomial bent functions with Niho exponents	92
5.4.3	Binomial bent functions with Dillon (like) exponents	94
	Bent functions via several Niho exponents	94
	Bent functions with multiple trace terms via Dillon (like) exponents . . .	94
5.4.4	Bent functions in hybrid form and Kerdock codes	94
6	Bent functions: secondary constructions	99
7	Bent functions: primary constructions (part II)	105
7.1	Primary bent functions with products of trace functions from a secondary construction and their duals	105
7.1.1	Infinite families of bent functions via Kasami function and Niho exponents, and their duals	110
7.1.2	Bent functions from the class of Maiorana-McFarland and their duals . .	113
7.1.3	An infinite family of bent functions from the Maiorana-McFarland completed class	118
7.1.4	An infinite family of cubic bent functions	119
7.2	Further constructions of infinite families of bent functions from new permutations and their duals	124
7.2.1	Further constructions of bent functions from new permutations and their duals	124
7.2.2	Further constructions of bent functions from secondary-like constructions of permutations	129
7.3	Infinite families of bent functions from involutions and their duals	134

8	Class \mathcal{H}, Niho bent functions and o-polynomials	139
8.1	Classes H and \mathcal{H} in bivariate form	139
8.1.1	Class H of Dillon	139
8.1.2	Class \mathcal{H}	140
8.2	Class \mathcal{H} in univariate form: Niho bent functions	142
8.2.1	A natural extension of class \mathcal{H}	142
8.2.2	Determining the duals of some bent functions in univariate form	143
	On the duals of the known binomial bent functions via Niho exponents	143
	On the duals of the known bent functions with 2^r Niho exponents	144
8.3	Functions in class \mathcal{H} and o-polynomials	146
8.3.1	O-equivalence	147
8.3.2	Niho Bent functions and Subiaco/Adelaide hyperovals	152
8.3.3	Bent functions from other o-polynomials	152
8.4	Some attempts to generalize the class \mathcal{H}	152
8.4.1	More \mathcal{H} -like bent functions	152
8.4.2	Class \mathcal{H} in characteristic p	152
9	Subclasses of bent functions: hyper-bent functions	155
9.1	Definitions and properties	155
9.2	Hyper-bent Boolean functions in symmetric cryptography	156
9.3	Hyper-bent Boolean functions in coding theory	156
9.3.1	Background on binary cyclic codes	156
9.3.2	Extended cyclic codes and hyper-bent functions	157
9.4	A characterization of hyper-bentness	157
9.5	Primary constructions and characterization of hyperbent functions in polynomial forms	158
9.5.1	Monomial hyper-bent functions via Dillon exponents	158
9.5.2	Binomial hyper-bent functions via Dillon (like) exponents	159
	A first family of binomial hyper-bent functions \mathfrak{F}_n	159
	A first family of binomial hyper-bent functions \mathfrak{F}_n : a generalization	163
	A first family of binomial hyper-bent functions \mathfrak{F}_n : a special case	165
	A second family of binomial hyper-bent functions \mathfrak{G}_n	173
	A third family of binomial hyper-bent functions	181
9.6	Hyper-bent functions from Boolean functions with the Walsh spectrum taking the same value twice	182
10	Hyper-bent functions: primary constructions with multiple trace terms	185
10.1	Hyper-bent functions with multiple trace terms via Dillon (like) exponents: the Charpin and Gong family	185
10.2	Hyper-bent functions with multiple trace terms via Dillon (like) exponents: the family \mathfrak{H}_n	186
10.2.1	Some conjectures: towards new hyper-bent functions	195
10.3	Hyper-bent functions with multiple trace terms via Dillon (like) exponents: the Wang et al. family	197
10.4	Hyper-bent functions via Dillon-like exponents: the general study	200
10.4.1	Extending the Charpin–Gong criterion	200
10.4.2	Hyper-bentness criterion for functions in \mathcal{H}_n	204
10.4.3	An alternate proof	208
10.5	Building infinite families of extension degrees	210

10.5.1	Prime case	210
10.5.2	Prime power case	212
10.5.3	Composite case	213
10.6	Applications	213
10.6.1	The case $b = 1$	213
	Prime case	214
	Prime power case	215
10.6.2	Explicit values for τ	216
	The case $\tau = 3$	217
	The case $\tau = 5$	218
	The case $\tau = 7$	219
	The case $\tau = 9$	219
	The case $\tau = 11$	224
	The case $\tau = 13$	225
	The case $\tau = 17$	225
	The case $\tau = 33$	226
11	(Hyper)-bent functions, exponential sums and (hyper-)elliptic curves	229
11.1	Elliptic curves and hyperelliptic curves	229
	11.1.1 Elliptic curves over finite fields	229
	11.1.2 Hyperelliptic curves and point counting	232
11.2	Exponential sums and algebraic varieties	233
	11.2.1 Kloosterman sums and elliptic curves	233
	11.2.2 Exponential sums and hyperelliptic curves	234
11.3	Efficient characterizations of hyper-bentness: reformulation in terms of cardinalities of curves	236
	11.3.1 Efficient characterizations of hyper-bentness: the Charpin and Gong criterion	236
	11.3.2 Efficient characterizations of hyper-bentness: our criterion	237
	11.3.3 Efficient characterizations of hyper-bentness: the Wang et al. criterion	242
	11.3.4 Algorithmic generation of hyper-bent functions in the family \mathcal{H}_n and hyperelliptic curves	245
	Characterizations in terms of hyperelliptic curves	246
	Asymptotic complexities	251
	Experimental results	252
11.4	Values of binary Kloosterman sums: some methods	257
	11.4.1 Divisibility of binary Kloosterman sums	257
	Classical results	257
	Using torsion of elliptic curves	258
	11.4.2 Finding specific values of binary Kloosterman sums	259
	Generic strategy	259
	Zeros of binary Kloosterman sums	259
	Implementation for the value 4	260
11.5	Bent functions and exponential sums	262
12	Bent vectorial functions	267
12.1	Bent vectorial functions	267
	12.1.1 Vectorial functions	267
	12.1.2 Vectorial functions that are bent	268
	12.1.3 Primary constructions of bent vectorial functions	269

12.1.4	On the (non-)existence of vectorial monomial bent functions of the form $Tr_r^n(ax^d)$ where r/n	275
12.1.5	Secondary constructions of bent vectorial functions	277
12.2	Vectorial bent functions and Kerdock codes	281
12.3	Hyper-bent vectorial functions	282
12.4	Bent Boolean functions associated to AB functions	283
13	Bent functions in arbitrary characteristic	287
13.1	On p -ary bent functions: generalities and constructions	287
13.1.1	Walsh transform of a p -ary function	287
13.1.2	Non-binary bent functions	288
13.2	Constructions of bent functions in arbitrary characteristic	288
13.2.1	Known primary constructions of bent Boolean functions: a summary	288
	Known infinite classes of bent functions in univariate trace form	289
	Known infinite classes of bent functions in bivariate trace form	291
13.2.2	Constructions of bent functions in odd characteristic	296
14	Bent functions and (partial-)spreads	303
14.1	Spread and partial spreads	303
14.1.1	Introduction to spread and partial spreads	303
14.1.2	Some classical examples of spreads	304
14.2	Bent functions from the Desarguesian spread	308
14.2.1	Bent functions whose restrictions to multiplicative cosets $u\mathbb{F}_{2^m}^*$ ($u \in U$) are constant	308
14.2.2	Bent functions whose restrictions to the m -spreads $u\mathbb{F}_{2^m}$ ($u \in U$) are linear	316
	An explicit example.	317
14.2.3	Bent functions whose restrictions to the multiplicative cosets $u\mathbb{F}_{2^m}^*$ ($u \in U$) are affine	320
14.3	Bent functions from other spreads	323
14.3.1	Bent functions from the class \mathcal{PS} -like	324
14.3.2	Bent functions which are linear on elements of classical spreads	326
14.4	Overview on constructions of bent functions linear on the elements of spreads	326
14.4.1	Bent functions linear on the elements of the Desarguesian spreads: the so-called class \mathcal{H}	326
14.4.2	Bent functions linear on the elements of other spreads: \mathcal{H} -like functions	327
	The case of André's spreads:	328
	The case of spreads based on prequasifields:	328
14.5	Bent functions linear on the elements of symplectic presemifields	330
14.5.1	Two explicit constructions	330
14.5.2	On oval polynomials for presemifields	333
14.6	Known vs. unknown bent functions	335
15	Various cryptographic and algebraic generalizations of bent functions	339
15.1	Partially bent functions	339
15.2	Rotation symmetric (RS) bent functions and idempotent bent functions	341
15.2.1	Rotation symmetric (RS) bent functions	342
15.2.2	Infinite classes of RS bent functions	342
15.2.3	Univariate RS functions (idempotents)	343
15.2.4	Idempotent bent functions and secondary constructions of rotation symmetric	344

Bivariate representation of idempotents	345
Weak idempotents and the related RS and weak RS functions	345
A secondary construction of RS and idempotent functions	346
15.2.5 A transformation on rotation symmetric bent functions	347
Relationship between the bentness of f and f'	348
15.3 Homogeneous bent functions	349
15.4 Generalized bent functions: the \mathbb{Z}_p -valued bent functions	350
15.5 Generalized bent functions from coding point of view	351
15.5.1 Galois ring	352
15.5.2 Generalized \mathbb{Z}_4 -valued bent functions	352
15.5.3 \mathbb{Z}_4 -valued quadratic forms	353
15.5.4 Generalized bent functions and \mathbb{Z}_4 -valued bent functions	354
15.6 \mathbb{Z} -bent functions	356
15.7 Negabent functions	357
15.8 Bent functions on a finite group	359
16 Plateaued functions: generalities and characterizations	365
16.1 Plateaued Boolean functions	365
16.1.1 Near-bent (1-plateaued functions)	366
16.1.2 Semi-bent (2-plateaued functions)	369
16.2 Special plateaued functions via linear translators	370
16.2.1 Constructions of bent and semi-bent Boolean functions from the class of Maiorana-McFarland using one linear structure	371
16.2.2 Constructions of bent and semi-bent Boolean functions from the class of Maiorana-McFarland using two linear structures	372
16.2.3 Constructions of bent and k -plateaued functions using linear translators	375
16.2.4 Bent functions not belonging to the class of Maiorana-McFarland using linear translators	376
16.2.5 A secondary construction of bent and semi-bent functions using derivatives and linear translators	380
16.2.6 A secondary construction of bent functions using certain quadratic and cubic functions together with linear structures	381
16.3 Various characterizations of plateaued functions in arbitrary characteristic	385
16.3.1 Characterizations of plateaued p -ary functions	386
16.3.2 Characterization of p -ary bent (0-plateaued) functions	392
16.4 Characterization of vectorial bent functions in arbitrary characteristic	396
16.5 Characterization of vectorial s -plateaued functions	399
17 Plateaued Boolean functions: constructions of semi-bent functions	407
17.1 Semi-bent functions: constructions and characterizations	408
17.1.1 On constructions of quadratic semi-bent functions	408
17.1.2 On constructions of semi-bent functions from bent functions	409
Primary constructions in univariate representation from Niho and Dillon bent functions	409
17.2 Explicit constructions of semi-bent functions in even dimension	409
17.2.1 Explicit constructions of semi-bent functions in univariate representation and their links with Kloosterman sums	409
17.2.2 Semi-bent functions in polynomial forms with multiple trace terms and their link with Dickson polynomials	418

17.3	Semi-bent functions with multiple trace terms and hyperelliptic curves	426
17.4	General constructions of semi-bent functions	429
17.4.1	Characterizations of semi-bent functions	429
17.4.2	Constructions of semi-bent functions	431
	Constructions in bivariate form	431
	Constructions in univariate form	432
17.5	Semi-bent functions (in even dimension): constructions and characterizations . .	435
17.5.1	On constructions of quadratic semi-bent functions	435
17.5.2	On constructions of semi-bent functions from bent functions	436
	Primary constructions in univariate representation from Niho and Dillon bent functions	436
	Primary constructions in bivariate representation from the class \mathcal{H} of bent functions	451
	A construction from bent functions via the indirect sum	452
	A simple construction of semi-bent functions from bent functions by field extension	453
	Construction of semi-bent functions from bent functions by considering their derivatives	453
17.5.3	A general construction of semi-bent functions based on Maiorana-McFarland's construction	453
17.5.4	A construction from APN functions	454
17.5.5	Several constructions from hyperovals and oval polynomials	455
17.5.6	Secondary constructions of semi-bent functions	457
18	Linear codes from bent, semi-bent and almost bent functions	461
18.1	Two generic constructions of linear codes from functions	462
18.2	Linear codes from bent functions based on the second generic construction	462
18.3	Linear codes from bent functions based on the first generic construction	465
18.4	Linear codes from semi-bent functions based on the second generic construction .	468
18.5	Linear codes from almost bent functions based on the second generic construction	469
	Index	473

Overview

Boolean functions are important objects in discrete mathematics. They play a role in mathematics and almost all the domains of computer science. In this book, we are mainly interested in their relationships with error-correcting codes and private-key cryptography. Mathematically, Boolean functions are mostly considered in this book in their univariate representations over finite fields. The theory of finite fields is a branch of modern algebra that has come to the fore in the last 60 years because of its diverse applications in combinatorics, coding theory, cryptology, among others.

The book is devoted to special families of Boolean functions which are viewed as important objects in combinatorics and the information theory framework (namely, cryptography and coding theory).

In fact, one of the most important cryptographic characteristics of a Boolean function is its nonlinearity. Most interest is attracted by the extremal nonlinear functions. *Bent functions* are maximally nonlinear Boolean functions with an even number of variables and are optimal combinatorial objects.

In the mathematical field of combinatorics, a bent function is a special type of Boolean function. Defined and named in the 1960's by Oscar Rothaus [3] in research not published until 1976, bent functions are so called because they are as different as possible from all linear and affine functions. The first paper on bent functions has been written in 1966 by O. Rothaus (as indicated by J. Dillon in his thesis), but its final version was published ten years later in [3]. The definition of bent function can be extended in several ways, leading to different classes of generalized bent functions that share many of the useful properties of the original.

Bent functions are wonderful creatures, initially studied by John Francis Dillon in his PhD thesis [2]. They have attracted a lot of research, especially in the last 20 years for their own sake as interesting combinatorial objects (e.g. difference sets), in design theory (any difference set can be used to construct a symmetric design) but also for their relations to coding theory (e.g. Reed-Muller codes, Kerdock codes, etc.) and applications in cryptography (design of stream ciphers) and sequence theory. A jubilee survey paper on bent functions giving an historical perspective, and making pertinent connections to designs, codes and cryptography is [1].

In cryptography, bent functions play a central role in the robustness of stream and block ciphers, since they are the only source of their nonlinearity, by providing confusion in these cryptosystems. The main cryptographic weaknesses of these functions in symmetric cryptography, forbidding to directly use them in stream ciphers, is that bentness makes it impossible for them to be balanced (that is, to have output uniformly distributed over the smallest field of cardinality 2); this induces a statistical correlation between the plaintext and the ciphertext.

A natural generalization of Boolean functions are the multi-output Boolean functions. Such vectorial functions constitute the so-called Substitution boxes (S-boxes) in symmetric cryptosystems which are fundamental parts of block ciphers. Bent vectorial functions can be involved in the substitution boxes (S-boxes) of block ciphers, whose role is also to bring some amount of

nonlinearity allowing them to resist differential and linear attacks.

Bent functions are particular plateaued functions. The notion of plateaued function has been introduced in 1999 by Zheng and Zhang as good candidates for designing cryptographic functions since they possess desirable various cryptographic characteristics. They are defined in terms of the Walsh-Hadamard spectrum. Plateaued functions bring together various nonlinear characteristics and include two important classes of Boolean functions defined in even dimension: the well-known bent functions and the semi-bent functions. Very recently, the study of semi-bent functions has attracted the attention of several researchers. Many progresses in the design of such functions have been made.

Bent functions, their subclasses (e.g. hyper-bent functions) and their generalizations (e.g. plateaued functions) have many theoretical and practical applications in combinatorics, coding theory, (symmetric) cryptography and sequence theory. Bent functions (including their constructions) have been extensively investigated since 1974. A complete classification of bent functions is elusive and looks hopeless today, therefore, not only their characterization, but also their generation are challenging problems.

The research activity on bent functions has been important for four decades and remains very intensive. However, very recently, many advances have been obtained on super classes of bent functions (plateaued functions, partially bent functions, etc), related classes of bent functions (semi-bent functions, near-bent functions, etc) and subclasses (hyper-bent functions, Niho bent functions, symmetric bent functions, bent nega-bent functions ect.). In particular, many new connections in the framework of semi-bent functions with other domains of mathematics and computer science (Dickson polynomial, Kloosterman sums, spreads, oval polynomial, finite geometry, coding, cryptography, sequences, etc) have been exhibited. The research in this framework is relatively new and becomes very active.

This book provides a detailed survey of main results in binary and generalized bent functions, presents a systematic overview of their generalizations, their variations, their applications, considers open problems in classification and systematization of bent functions, discusses proofs of several results and reflects recent developments and trends in the field. Up to now, there is no analog of this book in detail and completeness of material on bent functions, their variations and their generalizations. It is the first book in this field collecting essential material and is complementary to the existing surveys, since the emphasis is on bent functions via a univariate approach based on finite fields.

In this book we have aimed at presenting both the classical and the applications-oriented aspects of the subject. The reader will find many results and several techniques that are of importance. Because of the vastness of the subject, limitations had to be imposed on the choice of the material: we are mostly dealing with binary bent functions. The book tries to be as self-contained as possible. It contains information from highly regarded sources. Wide varieties of references are listed.

The book is split into 18 chapters. In most chapters, we bring some preliminaries providing enough background for the unfamiliar reader to understand the content of the chapter in which we present advanced results, significant advancements and the recent contributions of the researchers to the subject.

The noteworthy prerequisite for the book is a background in linear algebra and basic concepts in finite fields such as the general structure theory of finite fields, the theory of polynomials over finite fields and the theory of Boolean functions.

Chapter 1, is basic for the rest of the book as it contains the general notions related to Boolean functions as well as notions and concepts used throughout the book. In Chapter 2, we provide several technical results and some mathematical tools that we need subsequently in several chapters. Chapter 3 presents and discusses Boolean functions as important primitives of

symmetric cryptosystems playing a central role in their security. From chapter 4, we enter in the core of the main subject of the book. After a short historical note, we present definitions, main properties, classes and main constructions of binary bent functions as well as their relationship with error-correcting codes and private-key cryptography and combinatorics. Chapters 5, 6 and 7 are devoted to primary and secondary constructions of bent Boolean functions. In chapter 8, we will be interested in the connexion between the theory of bent functions and some important objects from finite geometry. Chapters 9, 10 and 11 concern a subclass of bent functions: the so-called hyper-bent functions. We shall show how we can treat the property of being hyperbent using tools from the theory of exponentials sums and the one of hyper-elliptic curves. Chapter 12 is dealing with multi-output bent functions. In chapter 13, we study bent functions in arbitrary characteristic. Chapter 14 deals with connections of bent functions and spreads. Chapter 15 is devoted to various cryptographic and algebraic generalizations of bent functions. We shall present partially bent functions, rotation symmetric bent functions, homogeneous bent functions, negabent functions and several generalized bent functions. Chapters 16 and 17 are concerned with the so-called plateaued functions which are cryptographic generalizations of bent functions. In particular, we discuss near and semi-bent functions. Finally, the last Chapter is devoted to recent advances related to linear error-correcting codes with few weights constructed via bent functions.

We hope that this book will be useful firstly to researchers in discrete mathematics and their applications in cryptography and coding theory; to students and professors of mathematical and theoretical computer science. It will also be useful to all interested in mathematical foundations of cryptography, engineers and managers in security. It can be used as a material for such university courses as discrete mathematics, Boolean functions, symmetric cryptography etc. The book will contain parts of different levels: from basic (available to students of the first year of Master) to very advanced (specialists in discrete mathematics, cryptography, coding theory, sequences, etc.).

This book is both a reader book on an exciting field and a reference of an extreme wealth. The *Notation* section can be found before the table of contents. An *Index* towards the end of this book gives some terms used. Readers are encouraged to send their comments to: smesnager@univ-paris8.fr

Acknowledgements. I am indebted to Gérard Cohen for his reading of the whole book, always in a cheerful manner, his very constructive and valuable comments, his interesting discussions on bent functions related to combinatorics and coding theory as well as his great support. I am very grateful to Claude Carlet. My meeting with him has completely changed my life as a researcher ! I never imagined finding so much energy and force in me to learn a new area just after my PhD thesis in algebra and modern algebraic geometry. I never forgot his encouragement and the interesting problems that he had suggested during my conversion from research in mathematics in algebra to discrete mathematics for cryptography and coding theory. I also thank him for his invitation to write together the jubilee survey on bent functions. Many thanks to Jean-Pierre Flori for his nice contribution and to Matthew Geoffrey Parker for his great contribution in writing Section ?? of Chapter ??. My gratitude to Joachim von zur Gathen, William M. Kantor, Henning Stichtenoth and Alev Topuzoglu for very interesting discussions and their support. I am grateful for help on various matters to Pascale Charpin, Cunsheng Ding, Tor Hellesteth, Harald Niederreiter and Ferruh Özbudak. I would like to thank also Kanat Abdukhalikov, Lilya Budaghyan, Anne Canteaut, Ayca Çeşmelioglu, Keqin Feng, Guang Gong, Alexander Kholosha, Gohar Kyureghyan, Gilles Lachaud, Philippe Langevin, Petr Lisoněk, Gary McGuire, Wilfried Meidl, Stanica Pantelimon, Enes Pasalic, Alexander Pott, François Rodier, Leo Storme, and Jacques Wolfmann for attractive discussions on bent functions during the redaction of this book.

Although I speak of its wonderful works in almost all my talks, I had never got the chance to meet John Dillon !

Bibliography

- [1] C. Carlet and S. Mesnager. Four decades of research on bent functions. In *Journal Designs, Codes and Cryptography*, Vol. 78, No. 1, pages 5–50, 2016. (Not cited.)
- [2] J. Dillon. Elementary Hadamard difference sets. In *PhD dissertation, University of Maryland*. (Not cited.)
- [3] O.S. Rothaus. On "bent" functions. In *J. Combin.Theory Ser A 20*, pages 300–305, 1976. (Not cited.)