Bent functions: fundamentals and results

Sihem Mesnager

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 (plateauted 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 Helleseth, Harald Niederreiter and Ferruh Özbudak. I would like to thank also Kanat Abdukhalikov, Lilya Budaghyan, Anne Canteaut, Ayca Ceşmelioğlu, 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.)