BENT FUNCTIONS

NATALIA TOKAREVA

RESULTS AND APPLICATIONS TO CRYPTOGRAPHY

Bent Functions

Results and Applications to Cryptography

by

Natalia Tokareva

Sobolev Institute of Mathematics

Novosibirsk State University

Novosibirsk, Russia

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Academic Press is an imprint of Elsevier

Academic Press is an imprint of Elsevier
125 London Wall, London, EC2Y 5AS, UK
525 B Street, Suite 1800, San Diego, CA 92101-4495, USA
225 Wyman Street, Waltham, MA 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-802318-1

Transferred to Digital Printing in 2015

Bent Functions

FOREWORD

Bent functions are fascinating mathematical objects. They were discovered by cryptographers who were searching for functions that are difficult to approximate by linear or affine functions. Bent functions are defined as functions that are at maximum distance to such weak functions. Bent functions were discovered independently by cryptographers in the US National Security Agency and in the Soviet Union; both nations decided to classify the results as confidential.

After one decade, Rothaus was allowed to publish his groundbreaking paper; it appeared in a journal on combinatorics in 1976. Around the same time (in 1972), Dillon published his seminal PhD thesis on elementary Hadamard difference sets. The first application area of bent functions considered in the open literature was coding theory. Academic cryptographers established the relation to cryptography only in 1989, when Meier and Staffelbach studied linear approximations of Boolean functions used in stream ciphers. This work stimulated broader interest in the topic, and inspired the author of this foreword to make some very modest contributions. Perhaps the largest impact on modern cryptography to date would be generated by the study of generalizations to vector Boolean functions that offer strong resistance against differential and linear attacks by Nyberg and others. This work resulted in the S-box used in the Advanced Encryption Standard (AES) that is today used in billions of devices. Other applications include wireless communications: sequences derived from bent functions can enhance code division multiple access (CDMA) transmission techniques.

Several years before Rothaus, Eliseev and Stepchenkov discovered bent functions in the USSR. Unfortunately their work is still classified as confidential. However, there is no doubt that the work of both authors inspired a large and valuable body of literature in Russian on the topic, some of which is public.

The author of this book has made a remarkable achievement. She has brought together the large body of knowledge on bent functions in both English and Russian in a single book. The book describes the history, presents definitions, and brings together all known results (125 theorems) and constructions in one integrated volume. It presents interesting perspectives based on the research of the author and a broad range of generalizations.

The literature in the first half century of bent functions is so vast that it is not possible to include the proofs. The book also contains many difficult open problems, enough to fill the careers of many mathematicians and cryptographers.

I hope that this book will inspire many researchers to explore the fascinating world of bent functions and to make progress on the rich and intricate problems in this world. I also hope that this book will increase mutual respect and understanding between researchers from the East and West and that it will lead to fruitful collaborations.

Bart Preneel
March 2015

PREFACE

Bent functions deserve
our bent to study them...

This book is devoted to such objects of discrete mathematics as Boolean *bent functions*. These functions have a remarkable property: each of them is at the maximal possible Hamming distance from the class of all affine Boolean functions. This extremal property distinguishes bent functions as the special mysterious class and leads to numerous applications of bent functions in combinatorics, coding theory, and cryptography.

Bent functions were introduced by O. Rothaus, an American mathematician, in the 1960s. At the same time, bent functions were studied in the USSR by V. A. Eliseev and O. P. Stepchenkov: they called such functions *minimal functions*. A little later J. A. Maiorana, R. L. McFarland, and J. Dillon proposed the first constructions of bent functions.

It was the early beginning...

The main goal of this book is to provide an overview of how the theory of bent functions developed from that time to this moment. This theory is still far from complete since too many questions remain open. We offer the most complete survey on bent functions. More than 125 theorems related to bent functions are included, and more than 400 references on bent functions are cited—from the very famous to very rare and widely unknown before. The book contains exclusive photographs of the first researchers in bent functions—most of them were never published before. Because of the large amount of work, not all important results are listed with the necessary details; some results are only mentioned, and we apologize for this limitation beforehand.

This book starts with basic definitions and historical aspects of the invention of bent functions. Applications of bent functions in cryptography (S-box construction, CAST, Grain, and HAVAL), discrete mathematics (Hadamard matrices, graphs, Kerdock codes, and bent codes) and communications (code division multiple access, bent sequences, and constant-amplitude codes) are discussed. We study basic properties of bent functions (degree restriction, affine transformations, rank, and duality) and equivalent representations of them (difference sets, designs, linear spreads, sets of subspaces, strongly regular graphs, and bent rectangles). Classifications of bent functions in a small number of variables are studied in detail (extended affine classification, classification in terms of bent rectangles, and graph classification for quadratic functions). An overview of algorithms for the generation of bent functions is presented.

Then we discuss combinatorial constructions of bent functions (simple iterative constructions, Maiorana-McFarland construction, partial spreads, Dillon's and Dobbertin's bent functions, minterm bent functions, and bent iterative functions). Then we come to relatively new algebraic constructions (Gold, Dillon, Kasami, Canteaut-Leander, and Canteaut-Charpin-Kuyreghyan bent exponents, and Niho bent functions) and discuss an algebraic approach in general. Connections between bent functions and other cryptographic properties (such as balancedness, correlation, and algebraic immunities) are also considered, together with some vectorial extensions.

Distances between bent functions are studied (minimal Hamming distance between bent functions, bounds on the number of bent functions at the minimal distance from a given one, locally metrical equivalence of bent functions, and the graph of minimal distances of bent functions). The group of automorphisms of the set of bent functions is established (it is proven that there are no other isometric mappings distinct from affine transformations that save the bent property of a function). Duality between the definitions of bent and affine functions is discussed.

Bounds on the number of bent functions are considered in detail. In our area of interest there are the best bounds for the number of bent functions up to 16 variables; for an arbitrary n, there is the best upper bound of C. Carlet and A. Klapper, and the best direct and iterative lower bounds of S. Agievich and the author, respectively. Hypotheses on the asymptotic value of the number of all bent functions are discussed. In connection with them the following question arises: Is it true that every Boolean function of degree up to $n/2$ can be represented as the sum of two bent functions? We consider this "bent sum decomposition problem" too, and prove that every Boolean function in n variables of a constant degree (less than or equal to $n/2$) can be represented as the sum of a constant number of bent functions in n variables.

Generalizations of bent functions with respect to their algebraic, combinatorial, and cryptographic properties are becoming more numerous and more widely studied from year to year. It is quite difficult not only to determine connections between generalizations, but also to collect information about all of them and provide a brief overview of the progress in this area. That is why a large part of this book is devoted to this theme. A systematic survey of the existing generalizations of bent functions and their known special subclasses is provided. Whenever possible we try to establish relations between various generalizations. We divide the generalizations into three groups: algebraic, combinatorial, and cryptographic. In the first group, we study q-valued bent functions, p-ary bent functions, bent functions over a finite field, generalized Boolean bent functions of Schmidt, bent functions from a finite Abelian group into the set of complex numbers on the unit circle, bent functions from a finite Abelian group into a finite Abelian group, non-Abelian bent functions, vectorial G-bent functions, and multidimensional bent functions on a finite Abelian group. In the second group, we deal with such generalizations and subclasses of bent functions as symmetric bent functions, homogeneous bent functions, rotation-symmetric bent functions, normal bent functions, self-dual and anti-self-dual bent functions, partially defined bent functions, plateaued functions, $\mathbb{Z}$-bent functions, and quantum bent functions. For the third, cryptographic, group in the sphere of our interest, there are semibent functions, balanced bent functions, partially bent functions, hyperbent functions, bent functions of higher order, and k-bent functions.

A large index completes the book. In general there are no proofs in the book: the huge volume of the results reviewed does not allow their inclusion. Moreover, we guess that there is no necessity in having proofs in such a book as this since many proofs are rather too special and will "slacken the pace" of an overview. There are only several proofs obtained by the author (automorphism group, bent iterative functions, etc.). But related to every result in this book we always include a reference to the original source. Thus, the interested reader can find all necessary details about the proofs.

I am very grateful to Mikhael M. Glukhov and Alexander V. Cheremushkin for their valuable advice related to this book and for providing me with several exclusive photographs of the first researchers of bent functions. I would like to honor the memory of Alexander A. Nechaev and express my deep gratitude to him for valuable discussions and support of the idea to write this book. My deep thanks go to Igor G. Shaposhnikov for providing me with the photographs of V. A. Eliseev and O. P. Stepchenkov. I express my gratitude to Sergey V. Agievich for several useful discussions. My kind thanks go to Alexander A. Evdokimov for his active support and a friendly atmosphere during the work. Finally, I thank Anastasia Gorodilova and Nikolay Kolomeec for their kind attention to this book and helpful remarks. This book was supported by the Sobolev Institute of Mathematics, Novosibirsk State University, and RFBR grants (projects 14-01-00507, 15-07-01328).

Finally, I wish good luck and inspiration to every researcher who is going to solve hard problems in bent functions or who is just thinking about this at the moment. Who knows, maybe bent functions are your bent!

Natalia Tokareva
Akademgorodok, Novosibirsk, Russia
February, 2015

NOTATION

p	a prime number (in most cases $p = 2$)
n	a natural number (usually even)
$\mathbb{F}_p$	the prime field, $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$
$\mathbb{F}_p^n$	the n-dimensional vector space over $\mathbb{F}_p$
$\mathbb{F}_{p^n}$	the finite field with p^n elements (also denoted $\mathrm{GF}(p^n)$)
$\mathbb{F}_{p^n}^*$	the set of all nonzero elements of the field $\mathbb{F}_{p^n}$
$\mathrm{Aut}(\mathbb{F}_{p^n})$	the *Galois group* of the field $\mathbb{F}_{p^n}$; that is, the group of all its automorphisms with respect to superposition
$\|M\|$	the size of the set M
$\gcd(a, b)$	the *greatest common divisor* of two numbers a and b
$\oplus$	the sum over $\mathbb{F}_2$ (XOR operation)
$x = (x_1, \ldots, x_n)$	a binary vector over $\mathbb{F}_2$ of length n
$x \oplus y$	the sum of two binary vectors over $\mathbb{F}_2$, $x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n)$
$\langle x, y \rangle$	the standard *inner product* of vectors, where $\langle x, y \rangle = x_1 y_1 \oplus \cdots \oplus x_n y_n$
$x \preccurlyeq y$	the *precedence relation*: $x \preccurlyeq y$ if and only if for all $i = 1, \ldots, n$ $x_i \leqslant y_i$ holds (i.e., *x is covered* by y)
$d(x, y)$	the *Hamming distance* between vectors x and y
$\mathrm{wt}(x)$	the *Hamming weight* of a vector x
$\mathrm{wt}(k)$	the *Hamming weight* of a number k; that is, the Hamming weight of its binary representation
$f : \mathbb{F}_2^n \to \mathbb{F}_2$	a *Boolean function* in n variables
$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$	a *vectorial Boolean function* in n variables
$\deg(f)$	the *degree* of a Boolean function
$\mathrm{ANF}(f)$	the *algebraic normal form* of a Boolean function
E^n	a *Boolean cube* of dimension n
$\mathrm{supp}(f)$	the *support* of a Boolean function f, where $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$
$\mathrm{dist}(f, g)$	the *Hamming distance* between functions f and g; that is, $\mathrm{dist}(f, g) = \|\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}\|$
$\mathrm{wt}(f)$	the *Hamming weight* of a function f, $\mathrm{wt}(f) = \|\mathrm{supp}(f)\|$;
$\mathrm{tr}(c)$	a *trace* function, $\mathrm{tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$, defined as $\mathrm{tr}(c) = c + c^2 + c^{2^2} + c^{2^3} + c^{2^4} + \cdots + c^{2^{n-1}}$;
$\mathrm{tr}_k^n(c)$	a *trace* function, $\mathrm{tr}_k^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, defined as $\mathrm{tr}_k^n(c) = c + c^{2^k} + c^{2^{2k}} + c^{2^{3k}} + \cdots + c^{2^{k(n/k-1)}}$
N_f	*nonlinearity* of a Boolean function; that is, $N_f = \min_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2} \mathrm{dist}(f, \ell_{a,b})$, where $\ell_{a,b}$ is affine
$W_f(y)$	the *Walsh-Hadamard coefficient* of a Boolean function

$\widetilde{f}$	a *dual* bent function to a bent function f
$\mathcal{B}_n$	the set of all bent functions in n variables
$\mathcal{BI}_n$	the set of all bent iterative functions in n variables
$\mathrm{Aut}(\mathcal{M})$	the *group of automorphisms* of a subset M of Boolean functions
$\mathrm{GA}(n)$	the *general affine group*
$G_f = G(\mathbb{F}_2^n, \mathrm{supp}(f))$	a *Cayley graph* of a Boolean function; there is an edge between x and y if $x \oplus y$ belongs to $\mathrm{supp}(f)$
$\mathcal{PS}$	*partial spread* bent functions

CONTENTS