



# BENT FUNCTIONS

NATALIA TOKAREVA

RESULTS AND APPLICATIONS  
TO CRYPTOGRAPHY



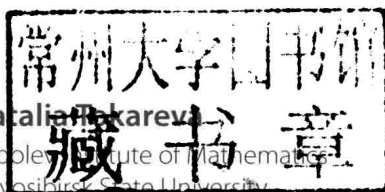
# Bent Functions

## Results and Applications to Cryptography

by

Natalia A. Pakareva

Sobolev Institute of Mathematics  
Novosibirsk State University  
Novosibirsk, Russia



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

Copyright © 2015 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

### Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

### 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

For information on all Academic Press publications  
visit our website at <http://store.elsevier.com/>



**Working together  
to grow libraries in  
developing countries**

[www.elsevier.com](http://www.elsevier.com) • [www.bookaid.org](http://www.bookaid.org)

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

$\tilde{f}$	a <i>dual</i> 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
$\text{Aut}(\mathcal{M})$	the <i>group of automorphisms</i> of a subset $M$ of Boolean functions
$\text{GA}(n)$	the <i>general affine group</i>
$G_f = G(\mathbb{F}_2^n, \text{supp}(f))$	a <i>Cayley graph</i> of a Boolean function; there is an edge between $x$ and $y$ if $x \oplus y$ belongs to $\text{supp}(f)$
$\mathcal{PS}$	<i>partial spread</i> bent functions

# CONTENTS

<i>Foreword</i>	<i>xi</i>
<i>Preface</i>	<i>xiii</i>
<i>Notation</i>	<i>xvii</i>
<b>1. Boolean Functions</b>	<b>1</b>
Introduction	1
1.1 Definitions	1
1.2 Algebraic normal form	3
1.3 Boolean cube and Hamming distance	4
1.4 Extended affinely equivalent functions	6
1.5 Walsh-Hadamard transform	7
1.6 Finite field and boolean functions	8
1.7 Trace function	9
1.8 Polynomial representation of a boolean function	11
1.9 Trace representation of a boolean function	11
1.10 Monomial boolean functions	14
<b>2. Bent Functions: An Introduction</b>	<b>17</b>
Introduction	17
2.1 Definition of a nonlinearity	17
2.2 Nonlinearity of a random boolean function	18
2.3 Definition of a bent function	18
2.4 If $n$ is odd?	20
2.5 Open problems	21
2.6 Surveys	23
<b>3. History of Bent Functions</b>	<b>25</b>
Introduction	25
3.1 Oscar Rothaus	25
3.2 V.A. Eliseev and O.P. Stepchenkov	26
3.3 From the 1970s to the present	28
<b>4. Applications of Bent Functions</b>	<b>31</b>
Introduction	31
4.1 Cryptography: linear cryptanalysis and boolean functions	31
4.2 Cryptography: one historical example	32

4.3	Cryptography: bent functions in CAST	34
4.4	Cryptography: bent functions in Grain	35
4.5	Cryptography: bent functions in HAVAL	36
4.6	Hadamard matrices and graphs	37
4.7	Links to coding theory	38
4.8	Bent sequences	39
4.9	Mobile networks, CDMA	40
4.10	Remarks	42
<b>5.</b>	<b>Properties of Bent Functions</b>	<b>43</b>
	Introduction	43
5.1	Degree of a bent function	43
5.2	Affine transformations of bent functions	44
5.3	Rank of a bent function	45
5.4	Dual bent functions	45
5.5	Other properties	46
<b>6.</b>	<b>Equivalent Representations of Bent Functions</b>	<b>49</b>
	Introduction	49
6.1	Hadamard matrices	49
6.2	Difference sets	49
6.3	Designs	50
6.4	Linear spreads	50
6.5	Sets of subspaces	51
6.6	Strongly regular graphs	52
6.7	Bent rectangles	52
<b>7.</b>	<b>Bent Functions with a Small Number of Variables</b>	<b>55</b>
	Introduction	55
7.1	Two and four variables	55
7.2	Six variables	56
7.3	Eight variables	59
7.4	Ten and more variables	60
7.5	Algorithms for generation of bent functions	61
7.6	Concluding remarks	62
<b>8.</b>	<b>Combinatorial Constructions of Bent Functions</b>	<b>63</b>
	Introduction	63
8.1	Rothaus's iterative construction	63
8.2	Maierana-McFarland class	64

8.3	Partial spreads: $\mathcal{PS}^+$ , $\mathcal{PS}^-$	65
8.4	Dillon's bent functions: $\mathcal{PS}_{\text{ap}}$	66
8.5	Dobbertin's construction	67
8.6	More iterative constructions	67
8.7	Minterm iterative constructions	68
8.8	Bent iterative functions: $\mathcal{BI}$	69
8.9	Other constructions	72
<b>9.</b>	<b>Algebraic Constructions of Bent Functions</b>	<b>73</b>
	Introduction	73
9.1	An algebraic approach	73
9.2	Bent exponents: general properties	74
9.3	Gold bent functions	75
9.4	Dillon exponent	76
9.5	Kasami bent functions	76
9.6	Canteaut-Leander bent functions (MF-1)	78
9.7	Canteaut-Charpin-Kuyreglyan bent functions (MF-2)	78
9.8	Niho exponents	79
9.9	General algebraic approach	80
9.10	Other constructions	80
<b>10.</b>	<b>Bent Functions and Other Cryptographic Properties</b>	<b>81</b>
	Introduction	81
10.1	Cryptographic criteria	81
10.2	High degree and balancedness	82
10.3	Correlation immunity and resiliency	82
10.4	Algebraic immunity	83
10.5	Vectorial bent functions, almost bent functions, and almost perfect nonlinear functions	85
<b>11.</b>	<b>Distances Between Bent Functions</b>	<b>89</b>
	Introduction	89
11.1	The minimal possible distance between bent functions	89
11.2	Classification of bent functions at the minimal distance from the quadratic bent function	90
11.3	Upper bound for the number of bent functions at the minimal distance from an arbitrary bent function	93
11.4	Bent functions at the minimal distance from a McFarland bent function	94
11.5	Locally metrically equivalent bent functions	94
11.6	The graph of minimal distances of bent functions	95



<b>12. Automorphisms of the Set of Bent Functions</b>	<b>97</b>
Introduction	97
12.1 Preliminaries	97
12.2 Shifts of the class of bent functions	98
12.3 Duality between definitions of bent and affine functions	102
12.4 Automorphisms of the set of bent functions	104
12.5 Metrically regular sets	105
<b>13. Bounds on the Number of Bent Functions</b>	<b>107</b>
Introduction	107
13.1 Preliminaries	107
13.2 The number of bent functions for small $n$	108
13.3 Upper bounds	108
13.4 Direct lower bounds	111
13.5 Iterative lower bounds	112
13.6 Lower bound from the bent iterative functions	114
13.7 Testing of the lower bound for small $n$	118
13.8 Asymptotic problem and hypotheses	120
<b>14. Bent Decomposition Problem</b>	<b>123</b>
Introduction	123
14.1 Preliminaries	123
14.2 Partial results	124
14.3 Boolean function as the sum of a constant number of bent functions	125
14.4 Any cubic boolean function in eight variables is the sum of at most four bent functions	127
14.5 Decomposition of dual bent functions	128
<b>15. Algebraic Generalizations of Bent Functions</b>	<b>133</b>
Introduction	133
15.1 Preliminaries	133
15.2 The $q$ -valued bent functions	134
15.3 The $p$ -ary bent functions	137
15.4 Bent functions over a finite field	139
15.5 Bent functions over quasi-frobenius local rings	141
15.6 Generalized boolean bent functions (of Schmidt)	141
15.7 Bent functions from a finite abelian group into the set of complex numbers on the unit circle	144
15.8 Bent functions from a finite abelian group into a finite abelian group	145
15.9 Non-abelian bent functions	147