Tor Helleseth
Dilip Sarwate
Hong-Yeop Song
Kyeongcheol Yang (Eds.)

Sequences and Their Applications – SETA 2004

LNCS 3486

Third International Conference
Seoul, Korea, October 2004
Revised Selected Papers

Springer

Tor Helleseth Dilip Sarwate
Hong-Yeop Song Kyeongcheol Yang (Eds.)

Sequences and Their Applications – SETA 2004

Third International Conference
Seoul, Korea, October 24-28, 2004
Revised Selected Papers

Springer

Volume Editors

Tor Helleseth
University of Bergen
Department of Informatics
Selmer Center, Thormohlensgate 55, 5020 Bergen, Norway
E-mail: tor.helleseth@ii.uib.no

Dilip Sarwate
University of Ilinois at Urbana-Champaign
Department of Electrical and Computer Engineering
1406 West Green Street, Urbana, IL 61801, USA
E-mail: sarwate@uiuc.edu

Hong-Yeop Song
Yonsei University
School of Electronics and Electrical Engineering
Seoul 120-749, Korea
E-mail: hy.song@coding.yonsei.ac.kr

Kyeongcheol Yang
Pohang University of Science and Technology
Department of Electronics and Electrical Engineering
Pohang, Kyungbuk 790-784, Korea
E-mail: kcyang@postech.ac.kr

Library of Congress Control Number: 2005925881

CR Subject Classification (1998): E.4, F.2, I.1, E.3, F.1, G.1

ISSN 0302-9743
ISBN-10 3-540-26084-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-26084-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11423461 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3486

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

This volume contains the refereed proceedings of the 3rd International Conference on Sequences and Their Applications (SETA 2004), held in Seoul, Korea during October 24–28, 2004. The previous two conferences, SETA 1998 and SETA 2001, were held in Singapore and Bergen, Norway, respectively. These conferences are motivated by the many widespread applications of sequences in modern communication systems. These applications include pseudorandom sequences in spread spectrum systems, code-division multiple-access, stream ciphers in cryptography and several connections to coding theory.

The Technical Program Committee of SETA 2004 received 59 submitted papers, many more than the submissions to previous SETA conferences. The Committee therefore had the difficult task of selecting the 33 papers to be presented at the Conference in addition to four invited papers. The authors of papers presented at the conference were invited to submit full papers that were refereed before appearing in this proceedings.

These proceedings have been edited by the Co-chairs of the Technical Program Committee for SETA 2004: Tor Helleseth of the University of Bergen, Norway, and Dilip Sarwate of the University of Illinois at Urbana-Champaign, USA, and Technical Program Committee members Hong-Yeop Song of Yonsei University, Korea, and Kyeongcheol Yang of Pohang University of Science and Technology, Korea. The editors wish to thank the other members of the Technical Program Committee: Serdar Boztas (Royal Melbourne Institute of Technology, Australia), Claude Carlet (INRIA and University of Paris 8, France), Zongduo Dai (University of Science and Technology of China, Beijing, China), Cunsheng Ding (Hong Kong University of Science and Technology, Hong Kong, China), Hans Dobbertin (Ruhr University Bochum, Germany), Pingzhi Fan (Southwest Jiaotong University, China), Solomon W. Golomb (University of Southern California, USA), Guang Gong (University of Waterloo, Canada), Tom Høholdt (Technical University of Denmark, Denmark), Andrew Klapper (University of Kentucky, USA), P. Vijay Kumar (University of Southern California, USA), Vladimir Levenshtein (Keldysh Institute of Applied Mathematics, Russia), Oscar Moreno (University of Puerto Rico, Puerto Rico), Harald Niederreiter (National University of Singapore, Singapore), Matthew Parker (University of Bergen, Norway), Kenneth G. Paterson (Royal Holloway, University of London, UK), Aleksander Pott (Otto von Guericke University Magdeburg, Germany), Hans Schotten (Qualcomm CDMA Technologies, Nürnberg, Germany), Patrick Sole (CNRS-I3S, ESSI, Sophia Antipolis, France), Naoki Suehiro (University of Tsukuba, Japan) for providing clear, insightful, and prompt reviews of the submitted papers.

In addition to the contributed papers, there were four invited papers. These papers provide an overview of new developments in some important areas related

to sequences. The invited papers by Jedwab and by Parker both include an updated overview and some recent results on the constructions of some exciting new families of sequences with a merit factor more than 6.3. Klapper gives an overview of the fascinating topic of feedback with carry shift registers, while Dobbertin and Leander present new and recent results on bent functions.

We wish to thank Jong-Seon No and Habong Chung for their support as General Co-chairs of SETA 2004; Dong-Joon Shin, Wonjin Sung and Jun Heo for their support as members of the Organizing Committee of SETA 2004. Last but not least, we thank all the authors of the papers presented at SETA 2004 for their help in making this conference a resounding success. Finally, we also thank the Korea Research Foundation (KTF) for its financial support.

March, 2005

Tor Helleseth
Dilip Sarwate
Hong-Yeop Song
Keongcheol Yang

Organization

SETA 2004

October 24–28, 2004, Seoul, Korea

General Co-chairs
Jong-Seon No, Seoul National University, Korea
Habong Chung, Hongik University, Korea

Program Co-chairs
Tor Helleseth, University of Bergen, Norway
Dilip Sarwate, University of Illinois at Urbana-Champaign, USA

Secretary and Treasury
Dong-Joon Shin, Hanyang University, Korea

Local Arrangements
Wonjin Sung, Sogang University, Korea

Registration
Jun Heo, Konkuk University, Korea

Publication Co-editors
Hong-Yeop Song, Yonsei University, Korea
Kyeongcheol Yang, POSTECH, Korea

Technical Program Committee for SETA 2004

Program Co-chairs

Tor Helleseth ..... University of Bergen, Norway
Dilip Sarwate ..... University of Illinois at Urbana-Champaign, USA

Program Committee

Serdar Boztas ..... RMIT University, Australia
Claude Carlet ..... INRIA and University of Paris 8, France
Zongduo Dai ..... University of Science and Technology of China, Beijing, China
Cunsheng Ding ... Hong Kong University of Science and Technology, Hong Kong, China
Hans Dobbertin ..... Ruhr University Bochum, Germany
Pingzhi Fan ..... Southwest Jiaotong University, China
Solomon W. Golomb ..... University of Southern California, USA
Guang Gong ..... University of Waterloo, Canada
Tom Høholdt ..... Technical University of Denmark, Denmark
Andrew Klapper ..... University of Kentucky, USA
P. Vijay Kumar ..... University of Southern California, USA
Vladimir Levenshtein ..... Keldysh Institute of Applied Mathematics, Russia
Oscar Moreno ..... University of Puerto Rico, Puerto Rico
Harald Niederreiter ..... National University of Singapore, Singapore
Matthew G. Parker ..... University of Bergen, Norway
Kenneth G. Paterson ..... Royal Holloway, University of London, UK
Alexander Pott ..... Otto von Guericke University Magdeburg, Germany
Hans Schotten ..... Qualcomm CDMA Technologies, Nürnberg, Germany
Patrick Solé ..... CNRS-I3S, ESSI, Sophia Antipolis, France
Hong-Yeop Song ..... Yonsei University, Korea
Naoki Suehiro ..... University of Tsukuba, Japan
Kyeongcheol Yang ..... Pohang University of Science and Technology, Korea

Lecture Notes in Computer Science

For information about Vols. 1–3400

please contact your bookseller or Springer

Vol. 3525: A.E. Abdallah, C.B. Jones, J.W. Sanders (Eds.), Communicating Sequential Processes. XIV, 321 pages. 2005.

Vol. 3517: H.S. Baird, D.P. Lopresti (Eds.), Human Interactive Proofs. IX, 143 pages. 2005.

Vol. 3516: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part III. LXIII, 1143 pages. 2005.

Vol. 3515: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part II. LXIII, 1101 pages. 2005.

Vol. 3514: V.S. Sunderam, G.D.v. Albada, P.M.A. Sloot, J.J. Dongarra (Eds.), Computational Science – ICCS 2005, Part I. LXIII, 1089 pages. 2005.

Vol. 3510: T. Braun, G. Carle, Y. Koucheryavy, V. Tsaoussidis (Eds.), Wired/Wireless Internet Communications. XIV, 366 pages. 2005.

Vol. 3508: P. Bresciani, P. Giorgini, B. Henderson-Sellers, G. Low, M. Winikoff (Eds.), Agent-Oriented Information Systems II. X, 227 pages. 2005. (Subseries LNAI).

Vol. 3503: S.E. Nikoletseas (Ed.), Experimental and Efficient Algorithms. XV, 624 pages. 2005.

Vol. 3502: F. Khendek, R. Dssouli (Eds.), Testing of Communicating Systems. X, 381 pages. 2005.

Vol. 3501: B. Kégl, G. Lapalme (Eds.), Advances in Artificial Intelligence. XV, 458 pages. 2005. (Subseries LNAI).

Vol. 3500: S. Miyano, J. Mesirov, S. Kasif, S. Istrail, P. Pevzner, M. Waterman (Eds.), Research in Computational Molecular Biology. XVII, 632 pages. 2005. (Subseries LNBI).

Vol. 3498: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part III. L, 1077 pages. 2005.

Vol. 3497: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. L, 947 pages. 2005.

Vol. 3496: J. Wang, X. Liao, Z. Yi (Eds.), Advances in Neural Networks – ISNN 2005, Part II. L, 1055 pages. 2005.

Vol. 3495: P. Kantor, G. Muresan, F. Roberts, D.D. Zeng, F.-Y. Wang, H. Chen, R.C. Merkle (Eds.), Intelligence and Security Informatics. XVIII, 674 pages. 2005.

Vol. 3494: R. Cramer (Ed.), Advances in Cryptology – EUROCRYPT 2005. XIV, 576 pages. 2005.

Vol. 3492: P. Blache, E. Stabler, J. Busquets, R. Moot (Eds.), Logical Aspects of Computational Linguistics. X, 363 pages. 2005. (Subseries LNAI).

Vol. 3489: G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 358 pages. 2005.

Vol. 3488: M.-S. Hacid, N.V. Murray, Z.W. Raś, S. Tsumoto (Eds.), Foundations of Intelligent Systems. XIII, 700 pages. 2005. (Subseries LNAI).

Vol. 3486: T. Helleseth, D. Sarwate, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications - SETA 2004. XII, 451 pages. 2005.

Vol. 3483: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part IV. XXVII, 1362 pages. 2005.

Vol. 3482: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part III. LXVI, 1340 pages. 2005.

Vol. 3481: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part II. LXIV, 1316 pages. 2005.

Vol. 3480: O. Gervasi, M.L. Gavrilova, V. Kumar, A. Laganà, H.P. Lee, Y. Mun, D. Taniar, C.J.K. Tan (Eds.), Computational Science and Its Applications – ICCSA 2005, Part I. LXV, 1234 pages. 2005.

Vol. 3479: T. Strang, C. Linnhoff-Popien (Eds.), Location- and Context-Awareness. XII, 378 pages. 2005.

Vol. 3477: P. Herrmann, V. Issarny, S. Shiu (Eds.), Trust Management. XII, 426 pages. 2005.

Vol. 3475: N. Guelfi (Ed.), Rapid Integration of Software Engineering Techniques. X, 145 pages. 2005.

Vol. 3468: H.W. Gellersen, R. Want, A. Schmidt (Eds.), Pervasive Computing. XIII, 347 pages. 2005.

Vol. 3467: J. Giesl (Ed.), Term Rewriting and Applications. XIII, 517 pages. 2005.

Vol. 3465: M. Bernardo, A. Bogliolo (Eds.), Formal Methods for Mobile Computing. VII, 271 pages. 2005.

Vol. 3463: M. Dal Cin, M. Kaâniche, A. Pataricza (Eds.), Dependable Computing - EDCC 2005. XVI, 472 pages. 2005.

Vol. 3462: R. Boutaba, K. Almeroth, R. Puigjaner, S. Shen, J.P. Black (Eds.), NETWORKING 2005. XXX, 1483 pages. 2005.

Vol. 3461: P. Urzyczyn (Ed.), Typed Lambda Calculi and Applications. XI, 433 pages. 2005.

Vol. 3460: Ö. Babaoglu, M. Jelasity, A. Montresor, C. Fetzer, S. Leonardi, A. van Moorsel, M. van Steen (Eds.), Self-star Properties in Complex Information Systems. IX, 447 pages. 2005.

Vol. 3459: R. Kimmel, N.A. Sochen, J. Weickert (Eds.), Scale Space and PDE Methods in Computer Vision. XI, 634 pages. 2005.

Vol. 3458: P. Herrero, M.S. Pérez, V. Robles (Eds.), Scientific Applications of Grid Computing. X, 208 pages. 2005.

Vol. 3456: H. Rust, Operational Semantics for Timed Systems. XII, 223 pages. 2005.

Vol. 3455: H. Treharne, S. King, M. Henson, S. Schneider (Eds.), ZB 2005: Formal Specification and Development in Z and B. XV, 493 pages. 2005.

Vol. 3454: J.-M. Jacquet, G.P. Picco (Eds.), Coordination Models and Languages. X, 299 pages. 2005.

Vol. 3453: L. Zhou, B.C. Ooi, X. Meng (Eds.), Database Systems for Advanced Applications. XXVII, 929 pages. 2005.

Vol. 3452: F. Baader, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XI, 562 pages. 2005. (Subseries LNAI).

Vol. 3450: D. Hutter, M. Ullmann (Eds.), Security in Pervasive Computing. XI, 239 pages. 2005.

Vol. 3449: F. Rothlauf, J. Branke, S. Cagnoni, D.W. Corne, R. Drechsler, Y. Jin, P. Machado, E. Marchiori, J. Romero, G.D. Smith, G. Squillero (Eds.), Applications of Evolutionary Computing. XX, 631 pages. 2005.

Vol. 3448: G.R. Raidl, J. Gottlieb (Eds.), Evolutionary Computation in Combinatorial Optimization. XI, 271 pages. 2005.

Vol. 3447: M. Keijzer, A. Tettamanzi, P. Collet, J.v. Hemert, M. Tomassini (Eds.), Genetic Programming. XIII, 382 pages. 2005.

Vol. 3444: M. Sagiv (Ed.), Programming Languages and Systems. XIII, 439 pages. 2005.

Vol. 3443: R. Bodik (Ed.), Compiler Construction. XI, 305 pages. 2005.

Vol. 3442: M. Cerioli (Ed.), Fundamental Approaches to Software Engineering. XIII, 373 pages. 2005.

Vol. 3441: V. Sassone (Ed.), Foundations of Software Science and Computational Structures. XVIII, 521 pages. 2005.

Vol. 3440: N. Halbwachs, L.D. Zuck (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XVII, 588 pages. 2005.

Vol. 3439: R.H. Deng, F. Bao, H. Pang, J. Zhou (Eds.), Information Security Practice and Experience. XII, 424 pages. 2005.

Vol. 3437: T. Gschwind, C. Mascolo (Eds.), Software Engineering and Middleware. X, 245 pages. 2005.

Vol. 3436: B. Bouyssounouse, J. Sifakis (Eds.), Embedded Systems Design. XV, 492 pages. 2005.

Vol. 3434: L. Brun, M. Vento (Eds.), Graph-Based Representations in Pattern Recognition. XII, 384 pages. 2005.

Vol. 3433: S. Bhalla (Ed.), Databases in Networked Information Systems. VII, 319 pages. 2005.

Vol. 3432: M. Beigl, P. Lukowicz (Eds.), Systems Aspects in Organic and Pervasive Computing - ARCS 2005. X, 265 pages. 2005.

Vol. 3431: C. Dovrolis (Ed.), Passive and Active Network Measurement. XII, 374 pages. 2005.

Vol. 3429: E. Andres, G. Damiand, P. Lienhardt (Eds.), Discrete Geometry for Computer Imagery. X, 428 pages. 2005.

Vol. 3428: Y.-J. Kwon, A. Bouju, C. Claramunt (Eds.), Web and Wireless Geographical Information Systems. XII, 255 pages. 2005.

Vol. 3427: G. Kotsis, O. Spaniol (Eds.), Wireless Systems and Mobility in Next Generation Internet. VIII, 249 pages. 2005.

Vol. 3423: J.L. Fiadeiro, P.D. Mosses, F. Orejas (Eds.), Recent Trends in Algebraic Development Techniques. VIII, 271 pages. 2005.

Vol. 3422: R.T. Mittermeir (Ed.), From Computer Literacy to Informatics Fundamentals. X, 203 pages. 2005.

Vol. 3421: P. Lorenz, P. Dini (Eds.), Networking - ICN 2005, Part II. XXXV, 1153 pages. 2005.

Vol. 3420: P. Lorenz, P. Dini (Eds.), Networking - ICN 2005, Part I. XXXV, 933 pages. 2005.

Vol. 3419: B. Faltings, A. Petcu, F. Fages, F. Rossi (Eds.), Constraint Satisfaction and Constraint Logic Programming. X, 217 pages. 2005. (Subseries LNAI).

Vol. 3418: U. Brandes, T. Erlebach (Eds.), Network Analysis. XII, 471 pages. 2005.

Vol. 3416: M. Böhlen, J. Gamper, W. Polasek, M.A. Wimmer (Eds.), E-Government: Towards Electronic Democracy. XIII, 311 pages. 2005. (Subseries LNAI).

Vol. 3415: P. Davidsson, B. Logan, K. Takadama (Eds.), Multi-Agent and Multi-Agent-Based Simulation. X, 265 pages. 2005. (Subseries LNAI).

Vol. 3414: M. Morari, L. Thiele (Eds.), Hybrid Systems: Computation and Control. XII, 684 pages. 2005.

Vol. 3412: X. Franch, D. Port (Eds.), COTS-Based Software Systems. XVI, 312 pages. 2005.

Vol. 3411: S.H. Myaeng, M. Zhou, K.-F. Wong, H.-J. Zhang (Eds.), Information Retrieval Technology. XIII, 337 pages. 2005.

Vol. 3410: C.A. Coello Coello, A. Hernández Aguirre, E. Zitzler (Eds.), Evolutionary Multi-Criterion Optimization. XVI, 912 pages. 2005.

Vol. 3409: N. Guelfi, G. Reggio, A. Romanovsky (Eds.), Scientific Engineering of Distributed Java Applications. X, 127 pages. 2005.

Vol. 3408: D.E. Losada, J.M. Fernández-Luna (Eds.), Advances in Information Retrieval. XVII, 572 pages. 2005.

Vol. 3407: Z. Liu, K. Araki (Eds.), Theoretical Aspects of Computing - ICTAC 2004. XIV, 562 pages. 2005.

Vol. 3406: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 829 pages. 2005.

Vol. 3404: V. Diekert, B. Durand (Eds.), STACS 2005. XVI, 706 pages. 2005.

Vol. 3403: B. Ganter, R. Godin (Eds.), Formal Concept Analysis. XI, 419 pages. 2005. (Subseries LNAI).

Vol. 3402: M. Daydé, J.J. Dongarra, V. Hernández, J.M.L.M. Palma (Eds.), High Performance Computing for Computational Science - VECPAR 2004. XI, 732 pages. 2005.

Vol. 3401: Z. Li, L.G. Vulkov, J. Waśniewski (Eds.), Numerical Analysis and Its Applications. XIII, 630 pages. 2005.

¥566.40元

Table of Contents

Invited Papers

Complexity of Sequences I

Complexity of Sequences II

Perfect Sequences

Sequence Constructions

Sequences over $\mathbb{Z}_m$

Sequence Generator Properties and Applications

Multi-dimensional Sequences

Optics and OFDM Applications

Polynomials and Functions

A Survey of Some Recent Results on Bent Functions

Hans Dobbertin and Gregor Leander

Department of Mathematics,
Ruhr-University Bochum,
D-44780 Bochum, Germany
{hans.dobbertin, gregor.leander}@ruhr-uni-bochum.de

Abstract. We report about recent results and methods in the study of bent functions. Here we focus on normality and trace expansions of bent functions.

1 Introduction

In this paper we present an overview about recent developments in the study of bent functions. We summarize and cite new results and techniques from the preprints [4, 10, 11, 15] and the paper [10].

Bent functions are maximally nonlinear Boolean functions with an even number of variables and were introduced by Rothaus [27] in 1976. Because of their own sake as interesting combinatorial objects, but also because of their relations to coding theory and applications in cryptography, they have attracted a lot of research, specially in the last ten years.

Despite their simple and natural definition, bent functions have turned out to admit a very complicated structure in general. On the other hand many special explicit constructions are known, primary ones giving bent functions from scratch and secondary ones building a new bent function from one or several given bent functions.

Normality of Bent Functions

Basic criteria of Boolean functions on $\mathbb{F}_2^n$, which are relevant to cryptography, are for instance its algebraic degree and nonlinearity. Another condition in this line of research is normality (resp. weak normality), i. e. the existence of a subspace of $\mathbb{F}_2^n$ with dimension $\frac{n}{2}$ such that the restriction of the given function is constant (resp. affine).

The notion of normality was introduced by the first author [16] in the study of bent functions and highly nonlinear balanced Boolean functions. While for increasing dimension n a counting argument can be used to prove that nearly all Boolean functions are non-normal, the situation for bent functions is more difficult. Most of the well studied families of bent functions are obviously normal and furthermore, unlike for arbitrary Boolean functions, normality has strong

T. Helleseth et al. (Eds.): SETA 2004, LNCS 3486, pp. 1–29, 2005.

consequences for the behavior of bent functions. One of the consequences is, that if a bent function f is constant on an $\frac{n}{2}$-dimensional affine subspace, then f is balanced on each proper coset. In other words, a normal bent function can be understood as a collection of balanced functions. The question whether non-normal bent functions exist at all, is therefore important. The interpretation of a normal bent function as a collection of balanced functions was used in [16] to give a framework for constructions of normal bent functions.

Monomial and Binomial Bent Functions

A complete classification of bent functions is elusive and looks hopeless today. In the second part of this paper we focus on traces of power functions, so called *monomial* Boolean functions. The study of trace expansions is well known in related areas, but has not yet been comprehensively studied for bent functions. This approach turns out to be very fruitful for several reasons. The only known non-normal bent functions are monomial bent functions, demonstrating that the study of monomial functions leads to new classes of bent functions. Furthermore one result of our considerations is, that for each of the well studied families of bent function, there is a monomial bent function belonging to these classes. Moreover, carefully studying the proofs for the monomial bent functions all these families can quite easily be rediscovered. In this sense most of the variety of (at least known) bent functions can already be discovered by the investigation of monomial functions.

In Section 5 we take the next step and extend our focus to linear combinations of two power functions. In particular we focus on Niho power functions, i.e. power functions where the restriction to the subfield of index 2 is linear. Using classical results for the Walsh-Spectrum of these functions and techniques recently developed by the first author, we present several new primary constructions of bent functions. These results are based on new techniques to study certain properties of rational functions. More precisely we present a general procedure to prove that certain rational functions induce one-to-one mappings.

These techniques and the Multivariate-Method developed by the first author (see [17]) follow the same line of reasoning. Both approaches are strongly based on properties of mappings, that can be defined in a global way, meaning that these properties are valid for an infinite chain of finite fields. In both situations this results in generic discussion of specific rational functions. These generic discussions are often relatively easy to describe for the conceptual point of view, while the actual inherent computations require the help of computer algebra. One key step is often to find the factorization of (parameterized) polynomials, which usually is not feasible by hand calculations. Nevertheless, once the factorization has been found, verifying the result is much easier and can here in most cases be done by hand.

2 Preliminaries

Throughout let $n = 2k$ be an even number. We recall some definitions and basic properties.

Walsh-Transform and Bent Functions
Given a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the function

$$a \in \mathbb{F}_2^n \mapsto f^{\mathcal{W}}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle a,x \rangle}$$

is called the *Walsh transform* of f. Moreover, the values $f^{\mathcal{W}}(a), a \in \mathbb{F}_2^n$ are called the Walsh coefficients of f. The set

$$\{f^{\mathcal{W}}(a), a \in \mathbb{F}_2^n\}$$

is called the Walsh-spectrum of f. Note that the Walsh-spectrum is not changed if we replace f by $f \circ H$ where H is a bijective affine or linear mapping, moreover adding an affine mapping does not change the absolute values of the Walsh-spectrum. Thus in most of our discussions we do not distinguish between these *affine* or *linear* equivalent functions.

By looking at the ± 1 valued function $F = (-1)^f$ the Walsh-transform of f corresponds (up to scaling) to the additive Fourier transform of F.

$$\hat{F} = 2^{-k} \sum_{x \in \mathbb{F}_2^n} F(x)(-1)^{\langle y,x \rangle}.$$

Due to the fact, that this transform is effected by the Hadamard matrix

$$\left((-1)^{\langle y,x \rangle}\right)_{x,y \in \mathbb{F}_2^n}$$

it is also sometimes called *Hadamard transform*. There are a few properties of the Hadamard transform, that we like to recall here.

For the operator $F \to \hat{F}$ we have the *involution law*

$$\hat{\hat{F}} = F$$

and with

$$(F * G)(x) = \sum_{u \in \mathbb{F}_2^n} F(u + x)G(x)$$

the *convolution law*

$$\widehat{F * G} = 2^k \hat{F}\hat{G}.$$

If we regard $\mathbb{R}^{\mathbb{F}_2^n}$ as an inner-product space where,

$$\langle F, G \rangle = \sum_{x \in \mathbb{F}_2^n} F(x)G(x)$$

the map $F \to \hat{F}$ is an orthogonal operator on $\mathbb{R}^{\mathbb{F}_2^n}$, i.e.

$$\sum_{x \in \mathbb{F}_2^n} F(x)G(x) = \sum_{y \in \mathbb{F}_2^n} \hat{F}(y)\hat{G}(y).$$