Lecture Notes in Computer Science 7280

Tor Helleseth Jonathan Jedwab (Eds.)

Sequences and Their Applications – SETA 2012

7th International Conference
Waterloo, ON, Canada, June 4-8, 2012
Proceedings

Springer

Volume Editors

Tor Helleseth
University of Bergen
Department of Informatics
P.O. Box 7803
5020 Bergen
Norway
E-mail: tor.helleseth@ii.uib.no

Jonathan Jedwab
Simon Fraser University
Department of Mathematics
8888 University Drive
Burnaby, BC, V5A 1S6
Canada
E-mail: jed@sfu.ca

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-30614-3 e-ISBN 978-3-642-30615-0
DOI 10.1007/978-3-642-30615-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012938265

CR Subject Classification (1998): G.2.1, E.3, C.2, K.6.5, D.4.6, J.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the refereed proceedings of the 7th International Conference on Sequences and Their Applications (SETA 2012) held in Waterloo, Canada, June 4–8, 2012. The previous six conferences were held in Singapore 1998, Bergen (Norway) 2001, Seoul (South Korea) 2004, Beijing (China) 2006, Lexington (USA) 2008, and Paris (France) 2010.

SETA 2012 invited submissions of previously unpublished work on technical aspects of sequences (one- and multi-dimensional) and their applications in communications, cryptography, coding, and combinatorics, including:

- Periodic and aperiodic correlation of sequences
- Synthesis and analysis of nonlinear feedback shift register sequences
- Linear and nonlinear complexity of sequences
- Boolean and vectorial functions
- Randomness properties of sequences
- Sequences for radar systems, including Costas arrays
- Sequences for OFDM, CDMA, and MIMO wireless communication
- Sequences for synchronization, identification, and hardware testing
- Sequences for network coding
- Sequences for stream ciphers and pseudorandom number generation
- Lightweight pseudorandom sequence generators for resource constrained devices

Invited talks were given by Rosemary A. Bailey (Queen Mary, University of London, UK), Charlie Colbourn (Arizona State University, USA), Thomas Johansson (Lund University, Sweden), Vahid Tarokh (Harvard University, USA), and Qing Xiang (University of Delaware, USA). A Special Session of the conference was held in honor of Solomon Golomb's 80th birthday. Our sincere thanks to the Program Committee for their dedication in the challenging task of refereeing 48 submissions and selecting 28 of these for presentation at the conference.

Special thanks to the General Chair Guang Gong and the Local Chair Xinxin Fan. We are grateful to Philip Regier and Fernando Rivero Hernandez for technical support, and Lisa Szepaniak for her constant support. Thanks to Kathy Holston for ensuring the smooth running of the conference and to Qi Chai for the design and hosting of the website of SETA 2012. We gratefully acknowledge the Department of Electrical and Computer Engineering of the University of Waterloo, the Fields Institute for Research in Mathematical Sciences (Toronto), the Mprime Network Inc., and the Ontario Research Fund Research Excellence (ORF-RE) program for their enthusiastic and generous financial support.

June 2012

Tor Helleseth
Jonathan Jedwab

Organization

General Chair

Guang Gong	University of Waterloo, Canada

Program Co-chairs

Tor Helleseth	University of Bergen, Norway
Jonathan Jedwab	Simon Fraser University, Canada

Local Chair

Xinxin Fan	University of Waterloo, Canada

Program Committee

Claude Carlet	University Paris 8, France
Agnes Chan	Northeastern University, USA
Pascale Charpin	INRIA, France
Jim Davis	University of Richmond, USA
Cunsheng Ding	Hong Kong University of Science and Technology, Hong Kong
Tuvi Etzion	Technion, Israel
Pingzhi Fan	Southwest Jiaotong University, China
Guang Gong	University of Waterloo, Canada
Tom Høholdt	Technical University of Denmark, Denmark
Honggang Hu	University of Science and Technology of China, China
Andrew Klapper	University of Kentucky, USA
P. Vijay Kumar	Indian Institute of Science, India
Wai Ho Mow	Hong Kong University of Science and Technology, Hong Kong
Jong-Seon No	Seoul National University, Korea
Udaya Parampalli	University of Melbourne, Australia
Matthew Parker	University of Bergen, Norway
Alexander Pott	Otto von Guericke University, Germany
Kai-Uwe Schmidt	Otto von Guericke University, Germany
Hong-Yeop Song	Yonsei University, Korea
Doug Stinson	University of Waterloo, Canada
Xiaohu Tang	Southwest Jiaotong University, China
Steve Wang	Carleton University, Canada
Arne Winterhof	Austrian Academy of Sciences, Austria

Kyeongcheol Yang	Pohang University of Science and Technology, Korea
Amr Youssef	Concordia University, Canada
Nam Yul Yu	Lakehead University, Canada

Sponsoring Institutions

Department of Electrical and Computer Engineering, University of Waterloo
The Fields Institute for Research in Mathematical Sciences, Toronto
The Mprime Network Inc.
The Ontario Research Fund Research Excellence

Table of Contents

Perfect Sequences

Odd Perfect Sequences and Sets of Spreading Sequences with Zero or Low Odd Periodic Correlation Zone 1
Yang Yang, Guang Gong, and Xiaohu Tang

Nonexistence of Certain Almost p-ary Perfect Sequences 13
Ferruh Özbudak, Oğuz Yayla, and C. Cengiz Yıldırım

Finite Fields

New Families of Differentially 4-Uniform Permutations over $\mathbb{F}_{2^{2k}}$ 25
Yin Tan, Longjiang Qu, Chik How Tan, and Chao Li

Dickson Polynomials, Hyperelliptic Curves and Hyper-bent Functions 40
Jean-Pierre Flori and Sihem Mesnager

Invited Paper

Variable Weight Sequences for Adaptive Scheduled Access in MANETs 53
Jonathan Lutz, Charles J. Colbourn, and Violet R. Syrotiuk

Boolean Functions

Arithmetic Walsh Transform of Quadratic Boolean Functions (Extended Abstract) 65
Andrew Klapper

Characterizing Negabent Boolean Functions over Finite Fields 77
Sumanta Sarkar

Computing the Weight of a Boolean Function from Its Algebraic Normal Form 89
Çağdaş Çalık and Ali Doğanaksoy

Boolean Functions Derived from Pseudorandom Binary Sequences 101
Gottlieb Pirsic and Arne Winterhof

Golomb 80th Birthday Session (I)

Infinite Sequences with Finite Cross-Correlation-II 110
Solomon W. Golomb

Irreducible Coefficient Relations 117
Thomas J. Dorsey and Alfred W. Hales

Wavelength Isolation Sequence Pairs 126
Jonathan Jedwab and Jane Wodlinger

Index Tables of Finite Fields and Modular Golomb Rulers............. 136
Ana Sălăgean, David Gardner, and Raphael Phan

Golomb 80th Birthday Session (II)

On the Aperiodic Hamming Correlation of Frequency-Hopping Sequences from Norm Functions 148
Zhengchun Zhou, Xiaohu Tang, Yang Yang, and Udaya Parampalli

Perfect Sequences of Unbounded Lengths over the Basic Quaternions ... 159
Santiago Barrera Acevedo and Thomas E. Hall

Linear Complexity

The Linear Complexity Deviation of Multisequences: Formulae for Finite Lengths and Asymptotic Distributions 168
Michael Vielhaber and Mónica del Pilar Canales Chacón

Linear Complexity of Binary Sequences Derived from Polynomial Quotients 181
Zhixiong Chen and Domingo Gómez-Pérez

Word-Oriented Transformation Shift Registers and Their Linear Complexity 190
Sartaj Ul Hasan, Daniel Panario, and Qiang Wang

Frequency Hopping

Low-Hit-Zone Frequency-Hopping Sequence Sets with New Parameters.. 202
Jin-Ho Chung and Kyeongcheol Yang

New Optimal Low Correlation Sequences for Wireless Communications 212
Oscar Moreno and Andrew Tirkel

Correlation of Sequences

Autocorrelation Properties of Some Pulse Compression Codes Derived from P3 and P4 Codes 224
Evgeny I. Krengel

On the d-ary Generalized Legendre-Sidelnikov Sequence 233
Ming Su

Invited Paper

Cyclotomy, Gauss Sums, Difference Sets and Strongly Regular Cayley Graphs 245
Qing Xiang

Bounds on Sequences

Partial Fourier Codebooks Associated with Multiplied Golay Complementary Sequences for Compressed Sensing 257
Xiao Bian and Nam Yul Yu

Welch Bound for Bandlimited and Timelimited Signals 269
Yutaka Jitsumatsu, Tohru Kohda, and Kazuyuki Aihara

Cryptography

Linear Weaknesses in T-functions 279
Tao Shi, Vladimir Anashin, and Dongdai Lin

Solving Compressed Right Hand Side Equation Systems with Linear Absorption 291
Thorsten Ernst Schilling and Håvard Raddum

Aperiodic Correlation

On Random Binary Sequences 303
Kai-Uwe Schmidt

The Density of Ternary Barker Sequences 315
Tomas Boothby

Walsh Transform

New Three-Valued Walsh Transforms from Decimations of Helleseth-Gong Sequences 327
Guang Gong, Tor Helleseth, Honggang Hu, and Chunlei Li

Author Index 339