Lecture Notes in Computer Science 6338

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

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max Planck Institute for Informatics, Saarbruecken, Germany

Claude Carlet   Alexander Pott (Eds.)

Sequences and Their Applications – SETA 2010

6th International Conference
Paris, France, September 13-17, 2010
Proceedings

Springer

Volume Editors

Claude Carlet
LAGA
Universities of Paris 8 and Paris 13
and CNRS, France
E-mail: claude.carlet@inria.fr

Alexander Pott
Institute for Algebra and Geometry
Otto-von-Guericke-University
Magdeburg, Germany
E-mail: alexander.pott@ovgu.de

Library of Congress Control Number: 2010934258

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

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

ISSN 0302-9743
ISBN-10 3-642-15873-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-15873-5 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

This volume contains the refereed proceedings of the *Sixth International Conference on Sequences and Their Applications (SETA 2010)*, held in Paris, France, September 13-17, 2010. The previous five conferences were held in Singapore (Republic of Singapore), Bergen (Norway), Seoul (South Korea), Beijing (China) and Lexington (USA). Topics of SETA include:

- Randomness of sequences
- Correlation (periodic and aperiodic types) and combinatorial aspects of sequences (difference sets)
- Sequences with applications in coding theory and cryptography
- Sequences over finite fields/rings/function fields
- Linear and nonlinear feedback shift register sequences
- Sequences for radar distance ranging, synchronization, identification, and hardware testing
- Sequences for wireless communication
- Pseudorandom sequence generators
- Boolean and vectorial functions for sequences, coding and/or cryptography
- Multidimensional sequences and their correlation properties
- Linear and nonlinear complexity of sequences

The Technical Program Committee of SETA 2010 refereed 56 submitted papers. Each paper was reviewed by at least 2 referees (at least 3 when an author was a TPC member) and the TPC selected 33 papers to be presented at the conference. In addition, we had 4 invited papers, by Robert Calderbank (Princeton University, USA), James Massey (retired from ETH Zurich, Switzerland), Jong-Seon No (Seoul National University, South Korea) and Arne Winterhof (Österreichische Akademie der Wissenschaften, Austria).

The Co-chairs of the TPC were Claude Carlet (Université Paris 8, France) and Alexander Pott (Otto-von-Guericke-Universität, Magdeburg, Germany). They wish to thank the other members of the Program Committee: Thierry P. Berger (Université de Limoges, France); Serdar Boztas (Royal Melbourne Institute of Technology, Australia); Lilya Budaghyan (University of Bergen, Norway); Pascale Charpin (INRIA, France) ; Gérard Cohen (Télécom ParisTech, France); Cunsheng Ding (Hong Kong University of Science and Technology, PR of China); Pingzhi Fan (Southwest Jiaotong University Chengdu, PR of China); Philippe Gaborit (Université de Limoges, France); Guang Gong (University of Waterloo, Canada); Tor Helleseth (University of Bergen, Norway); Jonathan Jedwab (Simon Fraser University, Canada); Thomas Johansson (Lund University, Sweden); Andrew Klapper (University of Kentucky, USA); Gohar Kyureghyan (Otto-von-Guericke-Universität, Germany); Gregor Leander (Technical University of Denmark); Wilfried Meidl (Sabanci University, Turkey); Sihem Mesnager (Université Paris 8, France); Gary McGuire (University College Dublin, Ireland);

Udaya Parampalli (University of Melbourne, Australia); Matthew Parker (University of Bergen, Norway); Bernhard Schmidt (Nanyang Technological University, Singapore, Republic of Singapore); Kai-Uwe Schmidt (Simon Fraser University, Canada); Hong-Yeop Song (Yonsei University, Korea); Kyeongcheol Yang (Pohang University of Science and Technology, Korea) and Nam Yul Yu (Lakehead University, Canada).

The editors are also grateful to Nina Brandstätter, Yuqing Chen, Jin-Ho Chung, Gary Greenfield, Yun Kyoung Han, Kathy Horadam, Honggang Hu, Ramakanth Kavuluru, Alexander Kholosha, Mels Kyuregyan, Petr Lisonek, Wai Ho Mow, Asha Rao, Xiaohu Tang, Andrew Turpin, Huaxiong Wang, Ruizhong Wei, Tony Wirth and Zhengchun Zhou for their help and assistance in the reviewing of papers.

We thank Springer for financing the best paper award, given by the Journal *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences* (CCDS) and awarded to the paper “Appended m-Sequences with Merit Factor Greater Than 3.34”, by Jonathan Jedwab and Kai-Uwe Schmidt.

We wish to thank Patrick Solé for his support as General Chair, Jean-Claude Belfiore for handling the EasyChair system, the webmaster Stephane Boucart, and Valérie Alidor, Nicolas Beaude (SEE), Danielle Childz, Zouina Sahnoune and Bruno Thedrez (Télécom ParisTech) for their kind help. Finally we would like to thank Télécom ParisTech for hosting the conference and Digiteo, CNRS and LAGA for their financial support.

September 2010

Claude Carlet
Alexander Pott

Table of Contents

Invited Paper

Low Correlation Zone Sequences 1
Jung-Soo Chung and Jong-Seon No

Algorithmic Aspects

Decimation Generator of Zadoff-Chu Sequences 30
Srdjan Budisin

An Algorithm for Constructing a Fastest Galois NLFSR Generating a Given Sequence 41
Jean-Michel Chabloz, Shohreh Sharif Mansouri, and Elena Dubrova

Acquisition Times of Contiguous and Distributed Marker Sequences: A Cross-Bifix Analysis 55
Čedomir Stefanović and Dragana Bajić

Frequency Hopping

Lower Bounds on the Average Partial Hamming Correlations of Frequency Hopping Sequences with Low Hit Zone 67
Xianhua Niu, Daiyuan Peng, and Fang Liu

New Families of Frequency-Hopping Sequences of Length mN Derived from the k-Fold Cyclotomy 76
Jin-Ho Chung and Kyeongcheol Yang

Multiple Access Systems

User-Irrepressible Sequences 88
Kenneth W. Shum, Yijin Zhang, and Wing Shing Wong

New Optimal Variable-Weight Optical Orthogonal Codes 102
Dianhua Wu, Jiayun Cao, and Pingzhi Fan

Invited Paper

Recent Results on Recursive Nonlinear Pseudorandom Number Generators 113
Arne Winterhof

Linear Complexity

A General Approach to Construction and Determination of the Linear Complexity of Sequences Based on Cosets 125
Ayça Çeşmelioğlu and Wilfried Meidl

On the Autocorrelation and the Linear Complexity of q-Ary Prime n-Square Sequences 139
Fang Liu, Daiyuan Peng, Xiaohu Tang, and Xianhua Niu

An Improved Approximation Algorithm for Computing the k-Error Linear Complexity of Sequences Using the Discrete Fourier Transform 151
Ana Sălăgean and Alexandra Alecu

Finite Fields

Transformations on Irreducible Binary Polynomials 166
Jean-Francis Michon and Philippe Ravache

Power Permutations in Dimension 32 181
Emrah ÇakÇak and Philippe Langevin

Character Sums

Multiplicative Character Sums with Counter-Dependent Nonlinear Congruential Pseudorandom Number Generators 188
Domingo Gomez

Ternary Kloosterman Sums Modulo 18 Using Stickelberger's Theorem 196
Faruk Göloğlu, Gary McGuire, and Richard Moloney

Merit Factor

Appended m-Sequences with Merit Factor Greater than 3.34 204
Jonathan Jedwab and Kai-Uwe Schmidt

FCSR

A With-Carry Walsh Transform (Extended Abstract) 217
Andrew Klapper and Mark Goresky

Clock-Controlled FCSR Sequence with Large Linear Complexity 229
Zhen Pan, Wei Su, and Xiaohu Tang

Vectorial Conception of FCSR 240
Abdelaziz Marjane and Boufeldja Allailou

Hadamard Matrices and Transforms

Fourier Duals of Björck Sequences 253
Branislav M. Popović

New Constructions of Complete Non-cyclic Hadamard Matrices, Related Function Families and LCZ Sequences 259
Krystal Guo and Guang Gong

Cryptography

$\mathbb{Z}_4$-Nonlinearity of a Constructed Quaternary Cryptographic Functions Class 270
Zoubida Jadda and Patrice Parraud

A Public Key Cryptosystem Based upon Euclidean Addition Chains.... 284
Fabien Herbaut and Pascal Véron

Optimal Authentication Codes from Difference Balanced Functions..... 298
Yang Yang, Xiaohu Tang, and Udaya Parampalli

Invited Paper

New Extensions and Applications of Welch-Bound-Equality Sequence Sets 305
James L. Massey

Statistical Analysis

Evaluation of Randomness Test Results for Short Sequences 309
Fatih Sulak, Ali Doğanaksoy, Barış Ege, and Onur Koçak

Statistical Analysis of Search for Set of Sequences in Random and Framed Data 320
Dragana Bajić and Čedomir Stefanović

Boolean Functions and Related Problems

On the Nonlinearity of Discrete Logarithm in $\mathbb{F}_{2^n}$ 333
Risto M. Hakala and Kaisa Nyberg

On a Conjecture about Binary Strings Distribution........ 346
Jean-Pierre Flori, Hugues Randriam, Gérard Cohen, and Sihem Mesnager

Nega–Hadamard Transform, Bent and Negabent Functions 359
Pantelimon Stănică, Sugata Gangopadhyay, Ankita Chaturvedi, Aditi Kar Gangopadhyay, and Subhamoy Maitra

Synchronization of Boolean Dynamical Systems: A Spectral Characterization 373
Jérémy Parriaux, Philippe Guillot, and Gilles Millérioux

Nonbinary Sequences

Some Constructions of Almost-Perfect, Odd-Perfect and Perfect Polyphase and Almost-Polyphase Sequences 387
Evgeny I. Krengel

Almost p-Ary Perfect Sequences 399
Yeow Meng Chee, Yin Tan, and Yue Zhou

Sequences, Bent Functions and Jacobsthal Sums 416
Tor Helleseth and Alexander Kholosha

Infinite Sequences

Infinite Sequences with Finite Cross-Correlation 430
Solomon W. Golomb

Invited Paper

Reed Muller Sensing Matrices and the LASSO 442
Robert Calderbank and Sina Jafarpour

Author Index 465