Lecture Notes in Computer Science 8865

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

Editorial Board

David Hutchison
Lancaster University, Lancaster, 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, Zürich, Switzerland

John C. Mitchell
Stanford University, Stanford, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Bern, Switzerland

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

Bernhard Steffen
TU Dortmund University, Dortmund, Germany

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
More information about this series at http://www.springer.com/series/7407
Preface

This volume contains the refereed proceedings of the Eighth International Conference on Sequences and Their Applications (SETA 2014) held in Melbourne, Australia, November 24–28, 2014. The previous seven conferences were held in Singapore 1998, Bergen (Norway) 2001, Seoul (South Korea) 2004, Beijing (China) 2006, Lexington (USA) 2008, Paris (France) 2010, and Waterloo (Canada) 2012.

SETA 2014 invited submissions of previously unpublished work on technical aspects of sequences and their applications in communications, cryptography, coding, and combinatorics, including:

- Randomness of sequences
- Aperiodic and periodic correlation of sequences
- Combinatorial aspects of sequences, including 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, synchronization, and identification
- Sequences for wireless communications
- Linear and nonlinear complexity of sequences
- Pseudorandom sequence generators
- Correlation and transformation of Boolean functions
- Multidimensional sequences and their correlation properties

Invited talks were given by Josef Dick (University of New South Wales, Australia), Tor Helleseth (University of Bergen, Norway), Kathy Horadam (RMIT University, Australia), and Bernhard Schmidt (Nanyang Technological University, Singapore).

The Program Committee of SETA 2014 has received 36 qualified submissions and each was refereed by at least two experts. The Program Committee selected 24 of them for presentation at the conference and for the inclusion in these proceedings. In addition, these proceedings contain two refereed invited papers, which are based on the talks given by Josef Dick and Kathy Horadam.

Our sincere thanks go to the Program Committee for their dedication in the challenging task of refereeing the submissions. Special thanks go to the General Chair, Udaya Parampalli.

We gratefully acknowledge the School of Engineering of the University of Melbourne and the Australian Mathematical Sciences Institute for their generous financial support.

November 2014

Kai-Uwe Schmidt
Arne Winterhof
Organization

General Chair

Udaya Parampalli University of Melbourne, Australia

Program Co-chairs

Kai-Uwe Schmidt Otto-von-Guericke University, Germany
Arne Winterhof Austrian Academy of Sciences, Austria

Program Committee

Christoph Aistleitner Technische Universität Graz, Austria
Serdar Boztas RMIT University, Australia
Claude Carlet University of Paris 8, France
Pascale Charpin Inria-Rocquencourt, France
Jim Davis University of Richmond, USA
Cunsheng Ding Hong Kong University of Science and Technology, Hong Kong
Tuvi Etzion Technion, Israel
Guang Gong University of Waterloo, Canada
Philip Hawkes Qualcomm, Australia
Honggang Hu University of Science and Technology of China, China
Tom Høholdt Technical University of Denmark, Denmark
Jonathan Jedwab Simon Fraser University, Canada
Alexander Kholosha University of Bergen, Norway
Andrew Klapper University of Kentucky, USA
Gohar Kyureghyan Otto-von-Guericke University, Germany
Wilfried Meidl Sabanci University, Turkey
Sihem Mesnager University of Paris 8, France
Wai Ho Mow Hong Kong University of Science and Technology, Hong Kong
Jong-Seon No Seoul National University, South Korea
Alina Ostafe University of New South Wales, Australia
Matthew Parker University of Bergen, Norway
Friedrich Pillichshammer Johannes Kepler Universität Linz, Austria
Alexander Pott Otto-von-Guericke University, Germany
Hong-Yeop Song Yonsei University, South Korea
Xiaohu Tang Southwest Jiaotong University, China
### Sponsoring Institutions

School of Engineering, University of Melbourne  
Australian Mathematical Sciences Institute
Contents

Invited Paper

Relationships Between CCZ and EA Equivalence Classes and Corresponding Code Invariants. ................................................................. 3
Kathy J. Horadam and Mercè Villanueva

Boolean Functions

Results on Constructions of Rotation Symmetric Bent and Semi-bent Functions ................................................................. 21
Claude Carlet, Guangpu Gao, and Wenfen Liu

Properties of a Family of Cryptographic Boolean Functions ............... 34
Qichun Wang and Chik How Tan

A New Transform Related to Distance from a Boolean Function (Extended Abstract) ................................................................. 47
Andrew Klapper

Constructing Hyper-Bent Functions from Boolean Functions with the Walsh Spectrum Taking the Same Value Twice ............... 60
Chunming Tang and Yanfeng Qi

Characterizations of Plateaued and Bent Functions in Characteristic $p$ ....... 72
Sihem Mesnager

Perfect Sequences

A Method of Optimisation of the Exhaustive Computer Search for Perfect Sequences ................................................................. 85
Oleg Kuznetsov

Almost Six-Phase Sequences with Perfect Periodic Autocorrelation Function ................................................................. 97
Vladimir E. Gantmakher and Mikhail V. Zaleshin

A Construction for Perfect Periodic Autocorrelation Sequences ........... 104
Samuel T. Blake and Andrew Z. Tirkel

A Simple Construction of Almost Perfect Quinary ASK and QAM Sequences ................................................................. 109
Guang Gong and Solomon Golomb
**Correlation of Arrays**

Inflation of Perfect Arrays Over the Basic Quaternions of Size $mn = (q + 1)/2$ ........................................... 123  
* Santiago Barrera Acevedo

Families of 3D Arrays for Video Watermarking ................................. 134  
* Sam Blake, Oscar Moreno, and Andrew Z. Tirkel

**Relative Difference Sets**

The Nonexistence of $(18, 3, 18, 6)$ Relative Difference Sets .................. 149  
* David Clark and Vladimir Tonchev

**Aperiodic Correlation**

Exhaustive Search for Optimal Minimum Peak Sidelobe Binary Sequences up to Length 80 ........................................... 157  
* Anatolii N. Leukhin and Egor N. Potekhin

**Invited Paper**

The Inverse of the Star-Discrepancy Problem and the Generation of Pseudo-Random Numbers ........................................... 173  
* Josef Dick and Friedrich Pillichshammer

**Pseudorandom Sequences and Stream Ciphers**

An Equivalence-Preserving Transformation of Shift Registers ................. 187  
* Elena Dubrova

A Lattice Rational Approximation Algorithm for AFSRs Over Quadratic Integer Rings ........................................... 200  
* Weihua Liu and Andrew Klapper

On the Lattice Structure of Inversive PRNG via the Additive Order ........... 212  
* Domingo Gómez-Pérez and Ana Gómez

Weaknesses in the Initialisation Process of the Common Scrambling Algorithm Stream Cipher ........................................... 220  
* Harry Bartlett, Ali Alhamdan, Leonie Simpson, Ed Dawson, and Kenneth Koon-Ho Wong

Distribution Properties of Half-$\ell$-Sequence ................................ 234  
* Ting Gu and Andrew Klapper
Crosscorrelation of Sequences

A Note on Cross-Correlation Distribution Between a Ternary \(m\)-Sequence and Its Decimated Sequence ........................................... 249
   Yongbo Xia, Tor Helleseth, and Gaofei Wu

Prime Numbers in Sequences

Conjectures Involving Sequences and Prime Numbers ................. 263
   Solomon Golomb

OFDM and CDMA

Optimal Sign Patterns for a Generalized Schmidl-Cox Method ........... 269
   Yutaka Jitsumatsu, Masahiro Hashiguchi, and Tatsuro Higuchi

A Novel Construction of Asymmetric Sequence Pairs Set with Zero-Correlation Zone .......................................................... 280
   Longye Wang, Xiaoli Zeng, and Hong Wen

Frequency-Hopping Sequences

On Low-Hit-Zone Frequency-Hopping Sequence Sets with Optimal Partial Hamming Correlation .............................................................. 293
   Hongyu Han, Daiyuan Peng, and Xing Liu

Improved Singleton Bound on Frequency Hopping Sequences ......... 305
   Xing Liu, Daiyuan Peng, and Hongyu Han

Author Index ................................................................. 315