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. Zaleshun

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 \( mn = (q + 1)/2 \)

*Santiago Barrera Acevedo*

Families of 3D Arrays for Video Watermarking

*Sam Blake, Oscar Moreno, and Andrew Z. Tirkel*

Relative Difference Sets

The Nonexistence of \( (18, 3, 18, 6) \) Relative Difference Sets

*David Clark and Vladimir Tonchev*

Aperiodic Correlation

Exhaustive Search for Optimal Minimum Peak Sidelobe Binary Sequences up to Length 80

*Anatolii N. Leukhin and Egor N. Potekhin*

Invited Paper

The Inverse of the Star-Discrepancy Problem and the Generation of Pseudo-Random Numbers

*Josef Dick and Friedrich Pillichshammer*

Pseudorandom Sequences and Stream Ciphers

An Equivalence-Preserving Transformation of Shift Registers

*Elena Dubrova*

A Lattice Rational Approximation Algorithm for AFSRs Over Quadratic Integer Rings

*Weihua Liu and Andrew Klapper*

On the Lattice Structure of Inversive PRNG via the Additive Order

*Domingo Gómez-Pérez and Ana Gómez*

Weaknesses in the Initialisation Process of the Common Scrambling Algorithm Stream Cipher

*Harry Bartlett, Ali Alhamdan, Leonie Simpson, Ed Dawson, and Kenneth Koon-Ho Wong*

Distribution Properties of Half-\( \ell \)-Sequence

*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
Sequences and Their Applications - SETA 2014
8th International Conference, Melbourne, VIC, Australia,
November 24-28, 2014, Proceedings
Schmidt, K.-U.; Winterhof, A. (Eds.)
2014, XI, 315 p. 25 illus., Softcover
ISBN: 978-3-319-12324-0