# Table of Contents

## Invited Papers

Shift Register Sequences – A Retrospective Account .......................... 1  
*Solomon W. Golomb*

The Probabilistic Theory of the Joint Linear Complexity  
of Multisequences .......................................................... 5  
*Harald Niederreiter*

Multi-Continued Fraction Algorithms and Their Applications  
to Sequences ............................................................... 17  
*Zongduo Dai*

Codes for Optical CDMA .................................................. 34  
*Reza Omrani, P. Vijay Kumar*

## Linear Complexity of Sequences

On the Linear Complexity of Sidel’nikov Sequences over $\mathbb{F}_d$ .......... 47  
*Nina Brandstätter, Wilfried Meidl*

Linear Complexity over $\mathbb{F}_p$ of Ternary Sidel’nikov Sequences .......... 61  
*Young-Sik Kim, Jung-Soo Chung, Jong-Seon No, Habong Chung*

Bounds on the Linear Complexity and the 1-Error Linear Complexity  
over $\mathbb{F}_p$ of M-ary Sidel’nikov Sequences .......................... 74  
*Jin-Ho Chung, Kyeongcheol Yang*

The Characterization of $2^n$-Periodic Binary Sequences with Fixed  
1-Error Linear Complexity ......................................... 88  
*Fang-Wei Fu, Harald Niederreiter, Ming Su*

## Correlation of Sequences

Crosscorrelation Properties of Binary Sequences with Ideal Two-Level  
Autocorrelation .......................................................... 104  
*Nam Yul Yu, Guang Gong*

Extended Hadamard Equivalence ........................................ 119  
*Doreen Hertel*
Analysis of Designing Interleaved ZCZ Sequence Families .............. 129
   Jin-Song Wang, Wen-Feng Qi

Stream Ciphers and Transforms

Security of Jump Controlled Sequence Generators for Stream Ciphers ............................................. 141
   Tor Helleseth, Cees J.A. Jansen, Shahram Khazaei, Alexander Kholosha

Improved Rijndael-Like S-Box and Its Transform Domain Analysis .... 153
   Seok-Yong Jin, Jong-Min Baek, Hong-Yeop Song

Topics in Complexities of Sequences

Nonlinear Complexity of Binary Sequences and Connections with Lempel-Ziv Compression ............................................. 168
   Konstantinos Limniotis, Nicholas Kolokotronis, Nicholas Kalouptsidis

On Lempel-Ziv Complexity of Sequences ..................... 180
   Ali Doğanaksoy, Faruk Göloğlu

Computing the k-Error N-Adic Complexity of a Sequence of Period $p^n$ .......................... 190
   Lihua Dong, Yupu Hu, Yong Zeng

On the Expected Value of the Joint 2-Adic Complexity of Periodic Binary Multisequences ......... 199
   Honggang Hu, Lei Hu, Dengguo Feng

Linear/Nonlinear Feedback Shift Register Sequences

On the Classification of Periodic Binary Sequences into Nonlinear Complexity Classes ............................................. 209
   George Petrides, Johannes Mykkeltveit

Sequences of Period $2^N - 2$ ............................................. 223
   Rainer Göttfert

A New Algorithm to Compute Remote Terms in Special Types of Characteristic Sequences ..................... 237
   Kenneth J. Giuliani, Guang Gong
## Multi-sequence Synthesis

Implementation of Multi-continued Fraction Algorithm and Application to Multi-sequence Linear Synthesis ........................................... 248
*Quanlong Wang, Kunpeng Wang, Zongduo Dai*

The Hausdorff Dimension of the Set of $r$-Perfect $M$-Multisequences ................................................................. 259
*Michael Vielhaber, Mónica del Pilar Canales Ch.*

## Filtering Sequences and Pseudorandom Sequence Generators

Lower Bounds on Sequence Complexity Via Generalised Vandermonde Determinants ................................................................. 271
*Nicholas Kolokotronis, Konstantinos Limniotis, Nicholas Kalouptsidis*

Construction of Pseudo-random Binary Sequences from Elliptic Curves by Using Discrete Logarithm ........................................... 285
*Zhixiong Chen, Shengqiang Li, Guozhen Xiao*

On the Discrepancy and Linear Complexity of Some Counter-Dependent Recurrence Sequences .................................................. 295
*Igor E. Shparlinski, Arne Winterhof*

## Sequences and Combinatorics

Nonexistence of a Kind of Generalized Perfect Binary Array .................. 304
*Zhang Xiyong, Guo Hua, Han Wenbao*

## FCSR Sequences

On the Distinctness of Decimations of Generalized $l$-Sequences .......... 313
*Hong Xu, Wen-Feng Qi*

On FCSR Memory Sequences ........................................................... 323
*Tian Tian, Wen-Feng Qi*

Periodicity and Distribution Properties of Combined FCSR Sequences ................................................................. 334
*Mark Goresky, Andrew Klapper*
### Aperiodic Correlation and Applications

Generalized Bounds on Partial Aperiodic Correlation of Complex Roots of Unity Sequences ........................................... 342  
*Lifang Feng, Pingzhi Fan*

Chip-Asynchronous Version of Welch Bound: Gaussian Pulse Improves BER Performance .................................................... 351  
*Yutaka Jitsumatsu, Tohru Kohda*

### Boolean Functions

On Immunity Profile of Boolean Functions ............................................ 364  
*Claude Carlet, Philippe Guillot, Sihem Mesnager*

Reducing the Number of Homogeneous Linear Equations in Finding Annihilators ................................................................. 376  
*Deepak Kumar Dalai, Subhamoy Maitra*

The Algebraic Normal Form, Linear Complexity and k-Error Linear Complexity of Single-Cycle T-Function ............................... 391  
*Wenying Zhang, Chuan-Kun Wu*

Partially Perfect Nonlinear Functions and a Construction of Cryptographic Boolean Functions ..................................................... 402  
*Lei Hu, Xiangyong Zeng*

Construction of 1-Resilient Boolean Functions with Very Good Nonlinearity ................................................................. 417  
*Soumen Maity, Chrisil Arackaparambil, Kezhasono Meyase*

### Author Index

................................................................. 433