

Solomon W. Golomb Matthew G. Parker
Alexander Pott Arne Winterhof (Eds.)

Sequences and Their Applications – SETA 2008

5th International Conference
Lexington, KY, USA, September 14-18, 2008
Proceedings

 Springer

Table of Contents

Probabilistic Methods and Randomness Properties of Sequences

Comparison of Point Sets and Sequences for Quasi-Monte Carlo and for Random Number Generation (Invited Paper)	1
<i>Pierre L'Ecuyer</i>	
On Independence and Sensitivity of Statistical Randomness Tests	18
<i>Meltem Sönmez Turan, Ali Doğanaksoy, and Serdar Boztaş</i>	
New Distinguishers Based on Random Mappings against Stream Ciphers	30
<i>Meltem Sönmez Turan, Çağdaş Çalık, Nurdan Buz Saran, and Ali Doğanaksoy</i>	
A Probabilistic Approach on Estimating the Number of Modular Sonar Sequences	42
<i>Ki-Hyeon Park and Hong-Yeop Song</i>	
A Study on the Pseudorandom Properties of Sequences Generated Via the Additive Order	51
<i>Honggang Hu and Guang Gong</i>	
On the Average Distribution of Power Residues and Primitive Elements in Inversive and Nonlinear Recurring Sequences	60
<i>Ayça Çeşmeliöğlü and Arne Winterhof</i>	

Correlation

Some Results on the Arithmetic Correlation of Sequences (Extended Abstract)	71
<i>Mark Goresky and Andrew Klapper</i>	
A Class of Nonbinary Codes and Sequence Families	81
<i>Xiangyong Zeng, Nian Li, and Lei Hu</i>	
Results on the Crosscorrelation and Autocorrelation of Sequences	95
<i>Faruk Göloğlu and Alexander Pott</i>	
m -Sequences of Lengths $2^{2k} - 1$ and $2^k - 1$ with at Most Four-Valued Cross Correlation	106
<i>Tor Helleseth and Alexander Kholosha</i>	

On the Correlation Distribution of Kerdock Sequences 121
Xiaohu Tang, Tor Helleseth, and Aina Johansen

Two New Families of Low-Correlation Interleaved QAM Sequences 130
Gagan Garg, P. Vijay Kumar, and C.E. Veni Madhavan

Combinatorial and Algebraic Foundations

The Combinatorics of Differentiation (Invited Paper) 142
Anna S. Bertiger, Robert J. McEliece, and Sarah Sweatlock

Group Representation Design of Digital Signals and Sequences 153
Shamgar Gurevich, Ronny Hadani, and Nir Sochen

Projective de Bruijn Sequences 167
Yuki Ohtsuka, Makoto Matsumoto, and Mariko Hagita

Multiplicative Character Sums of Recurring Sequences with Rédei Functions 175
Domingo Gomez and Arne Winterhof

On the Connection between Kloosterman Sums and Elliptic Curves 182
Petr Lisoněk

A Class of Optimal Frequency Hopping Sequences Based upon the Theory of Power Residues 188
Daiyuan Peng, Tu Peng, Xiaohu Tang, and Xianhua Niu

Security Aspects of Sequences

Sequences, DFT and Resistance against Fast Algebraic Attacks (Invited Paper) 197
Guang Gong

Expected π -Adic Security Measures of Sequences (Extended Abstract) 219
Andrew Klapper

Distance-Avoiding Sequences for Extremely Low-Bandwidth Authentication 230
Michael J. Collins and Scott Mitchell

On the Number of Linearly Independent Equations Generated by XL ... 239
Sondre Rønjom and Håvard Raddum

2^n -Periodic Binary Sequences with Fixed k -Error Linear Complexity for $k = 2$ or 3 252
Ramakanth Kavuluru

Generalized Joint Linear Complexity of Linear Recurring Multisequences	266
<i>Wilfried Meidl and Ferruh Özbudak</i>	

Algorithms

A Lattice-Based Minimal Partial Realization Algorithm	278
<i>Li-Ping Wang</i>	
A Fast Jump Ahead Algorithm for Linear Recurrences in a Polynomial Space	290
<i>Hiroshi Haramoto, Makoto Matsumoto, and Pierre L'Ecuyer</i>	
Parallel Generation of ℓ -Sequences	299
<i>Cédric Lauradoux and Andrea Röck</i>	

Correlation of Sequences over Rings

Design of M -Ary Low Correlation Zone Sequence Sets by Interleaving	313
<i>Jin-Ho Chung and Kyeongcheol Yang</i>	
The Peak to Sidelobe Level of the Most Significant Bit of Trace Codes over Galois Rings	322
<i>Patrick Solé and Dimitrii Zinoviev</i>	
On Partial Correlations of Various \mathbf{Z}_4 Sequence Families	332
<i>Paramalli Udaya and Serdar Boztas</i>	

Nonlinear Functions over Finite Fields

On the Higher Order Nonlinearities of Boolean Functions and S-Boxes, and Their Generalizations (Invited Paper)	345
<i>Claude Carlet</i>	
On a Class of Permutation Polynomials over \mathbb{F}_{2^n}	368
<i>Pascale Charpin and Gohar M. Kyureghyan</i>	
On 3-to-1 and Power APN S-Boxes	377
<i>Deepak Kumar Dalai</i>	
Negabent Functions in the Maiorana–McFarland Class	390
<i>Kai-Uwe Schmidt, Matthew G. Parker, and Alexander Pott</i>	
New Perfect Nonlinear Multinomials over $\mathbb{F}_{p^{2k}}$ for Any Odd Prime p ...	403
<i>Lilya Budaghyan and Tor Helleseth</i>	

A New Tool for Assurance of Perfect Nonlinearity 415
Nuray At and Stephen D. Cohen

Author Index 421