

Table of Contents

Invited Contributions

The Ubiquity of Reed-Muller Codes	1
<i>J.L. Massey (ETH-Zürich and Lund Univ.)</i>	
Self-dual Codes-Theme and Variations	13
<i>V. Pless (Univ. of Illinois)</i>	
Design of Differential Space-Time Codes Using Group Theory	22
<i>A. Shokrollahi (Digital Fountain)</i>	
Ideal Error-Correcting Codes: Unifying Algebraic and Number-Theoretic Algorithms	36
<i>M. Sudan (MIT)</i>	

Block Codes

Self-dual Codes Using Image Restoration Techniques	46
<i>A. Baliga (RMIT Univ.) and J. Chua (Monash Univ.)</i>	
Low Complexity Tail-Biting Trellises of Self-dual Codes of Length 24, 32 and 40 over $GF(2)$ and \mathbb{Z}_4 of Large Minimum Distance	57
<i>E. Cadic (France Telecom R&D), J.C. Carlach (France Telecom R&D), G. Olocco (Univ. Paris-Sud), A. Otmani (Univ. Limoges), and J.P. Tillich (Univ. Paris-Sud)</i>	
F_q -Linear Cyclic Codes over F_{q^m} : DFT Characterization	67
<i>B.K. Dey and B.S. Rajan (Indian Inst. of Science)</i>	

Code Constructions

Cyclic Projective Reed-Muller Codes	77
<i>T.P. Berger and L. de Maximy (Univ. Limoges)</i>	
Codes Identifying Sets of Vertices	82
<i>T. Laihonon and S. Ranto (Univ. Turku)</i>	
Duality and Greedy Weights of Linear Codes and Projective Multisets	92
<i>H.G. Schaathun (Univ. Bergen)</i>	

Codes and Algebra: Rings and Fields

Type II Codes over \mathbb{F}_{2^r}	102
<i>K. Betsumiya (Nagoya Univ.), M. Harada (Yamagata Univ.), and A. Munemasa (Kyushu Univ.)</i>	
On Senary Simplex Codes	112
<i>M.K. Gupta (Univ. Canterbury), D.G. Glynn (Univ. Canterbury), and T.A. Gulliver (Univ. Victoria)</i>	
Optimal Double Circulant \mathbb{Z}_4 -Codes	122
<i>T.A. Gulliver (Univ. Victoria) and M. Harada (Yamagata Univ.)</i>	
Constructions of Codes from Number Fields	129
<i>V. Guruswami (MIT)</i>	
On Generalized Hamming Weights for Codes over Finite Chain Rings	141
<i>H. Horimoto (Kumamoto Nat'l. Coll. of Tech.) and K. Shiromoto (Kumamoto Univ.)</i>	
Information Rates and Weights of Codes in Structural Matrix Rings	151
<i>A. Kelarev (Univ. Tasmania) and O. Sokratova (Univ. Tartu)</i>	

Codes and Algebra: Algebraic Geometry Codes

On Hyperbolic Codes	159
<i>O. Geil (Aalborg Univ.) and T. Høholdt (Tech. Univ. of Denmark)</i>	
On Fast Interpolation Method for Guruswami-Sudan List Decoding of One-Point Algebraic-Geometry Codes	172
<i>S. Sakata (Univ. Electro-Communications)</i>	
Computing the Genus of a Class of Curves	182
<i>M.C. Rodríguez-Palánquez, L.J. García-Villalba, and I. Luengo-Velasco (UCM Madrid)</i>	

Sequences

Iterations of Multivariate Polynomials and Discrepancy of Pseudorandom Numbers	192
<i>J. Gutierrez and D. Gomez-Perez (Univ. Cantabria)</i>	
Even Length Binary Sequence Families with Low Negaperiodic Autocorrelation	200
<i>M.G. Parker (Univ. Bergen)</i>	
On the Non-existence of (Almost-)Perfect Quaternary Sequences	210
<i>P. Parraud (Écoles Militaires St Cyr-Coëtquidan)</i>	

Maximal Periods of $x^2 + c$ in \mathbb{F}_q	219
<i>A. Peinado (Univ. Málaga), F. Montoya (CSIC), J. Muñoz (CSIC), and A.J. Yuste (Univ. Jaen)</i>	
On the Aperiodic Correlation Function of Galois Ring m -Sequences	229
<i>P. Udaya (Univ. Melbourne) and S. Boztas (RMIT Univ.)</i>	
Euclidean Modules and Multisequence Synthesis	239
<i>L. Wang (Univ. Sci. and Tech. of China)</i>	

Cryptography

On Homogeneous Bent Functions	249
<i>C. Charney (Univ. Melbourne and Univ. Karlsruhe), M. Rötteler (Univ. Karlsruhe), and T. Beth (Univ. Karlsruhe)</i>	
Partially Identifying Codes for Copyright Protection	260
<i>S. Encheva (HSH, Norway) and G. Cohen (ENST)</i>	
On the Generalised Hidden Number Problem and Bit Security of XTR ...	268
<i>I.E. Shparlinski (Macquarie Univ.)</i>	
CRYPTIM: Graphs as Tools for Symmetric Encryption	278
<i>V. Ustimenko (Univ. South Pacific)</i>	

Algorithms

An Algorithm for Computing Cocyclic Matrices Developed over Some Semidirect Products	287
<i>V. Álvarez, J.A. Armario, M.D. Frau, and P. Real (Univ. Sevilla)</i>	
Algorithms for Large Integer Matrix Problems	297
<i>M. Giesbrecht (Univ. Western Ontario), M. Jacobson, Jr. (Univ. Manitoba), and A. Storjohann (Univ. Western Ontario)</i>	
On the Identification of Vertices and Edges Using Cycles	308
<i>I. Honkala (Univ. Turku), M.G. Karpovsky (Boston Univ.), and S. Litsyn (Tel-Aviv Univ.)</i>	

Algorithms: Decoding

On Algebraic Soft Decision Decoding of Cyclic Binary Codes	315
<i>V.B. Balakirsky (Eindhoven Univ. of Technology)</i>	
Lifting Decoding Schemes over a Galois Ring	323
<i>E. Byrne (Nat'l. Univ. Ireland, Cork)</i>	

Sufficient Conditions on Most Likely Local Sub-codewords
in Recursive Maximum Likelihood Decoding Algorithms 333
T. Kasami (Hiroshima City Univ.), H. Tokushige (Hiroshima City Univ.), and Y. Kaji (Nara Inst. Science and Technology)

A Unifying System-Theoretic Framework
for Errors-and-Erasures Reed-Solomon Decoding 343
*M. Kuijper (Univ. Melbourne), M. van Dijk (Philips Research),
H. Hollmann (Philips Research), and J. Oostveen (Philips Research)*

An Algorithm for Computing Rejection Probability of MLD
with Threshold Test over BSC 353
T. Wadayama (Okayama Prefectural Univ.)

Algebraic Constructions

Cartan's Characters and Stairs of Characteristic Sets 363
F. Boulier and S. Neut (Univ. Lille I)

On the Invariants of the Quotients of the Jacobian
of a Curve of Genus 2 373
P. Gaudry and É. Schost (École Polytechnique)

Algebraic Constructions for PSK Space-Time Coded Modulation 387
*A.M. Gidi (Inst. Telecommunications Research), A.J. Grant
(Inst. Telecommunications Research), and S.S. Pietrobon (Small World Communications)*

Author Index 397

Applied Algebra, Algebraic Algorithms and
Error-Correcting Codes

14th International Symposium, AAECC-14, Melbourne,
Australia, November 26-30, 2001. Proceedings

Boztas, S.; Shparlinski, I.E. (Eds.)

2001, XII, 404 p., Softcover

ISBN: 978-3-540-42911-1