

Table of Contents

Invited Talks

Codes on Graphs: A Survey for Algebraists	1
<i>G. David Forney, Jr.</i>	
RA Codes Achieve AWGN Channel Capacity	10
<i>Hui Jin and Robert J. McEliece</i>	
Monomial Ideals and Planar Graphs	19
<i>Ezra Miller and Bernd Sturmfels</i>	
A Fast Program Generator of Fast Fourier Transforms	29
<i>Michael Clausen and Meinard Müller</i>	
On Integer Programming Problems Related to Soft-Decision Iterative Decoding Algorithms	43
<i>Tadao Kasami</i>	
Curves with Many Points and Their Applications	55
<i>Ian F. Blake</i>	

Codes and Iterative Decoding

New Sequences of Linear Time Erasure Codes Approaching the Channel Capacity	65
<i>M. Amin Shokrollahi</i>	
On the Theory of Low-Density Convolutional Codes	77
<i>Karin Engdahl, Michael Lentmaier, and Kamil Sh. Zigangirov</i>	

Combinatorics I: Arithmetic

On the Distribution of Nonlinear Recursive Congruential Pseudorandom Numbers of Higher Orders	87
<i>Frances Griffin, Harald Niederreiter, and Igor E. Shparlinski</i>	
A New Representation of Boolean Functions	94
<i>Claude Carlet and Philippe Guillot</i>	

Combinatorics II: Graphs and Matrices

An Algorithm to Compute a Nearest Point in the Lattice A_n^*	104
<i>I. Vaughan and L. Clarkson</i>	

Sequences from Cocycles	121
<i>Kathy J. Horadam</i>	

Block Codes I

On the Second Greedy Weight for Binary Linear Codes.	131
<i>Wende Chen and Torleiv Kløve</i>	

On the Size of Identifying Codes	142
<i>Uri Blass, Iiro Honkala, and Simon Litsyn</i>	

Algebra I: Rings and Fields

Fast Quantum Fourier Transforms for a Class of Non-abelian Groups	148
<i>Markus Püschel, Martin Rötteler, and Thomas Beth</i>	

Linear Codes and Rings of Matrices	160
<i>M. Greferath and S.E. Schmidt</i>	

On \mathbb{Z}_4 -Simplex Codes and Their Gray Images	170
<i>Mahesh C. Bhandari, Manish K. Gupta, and Arbind K. Lal</i>	

Decoding Methods

Some Results on Generalized Concatenation of Block Codes	181
<i>M. Bossert, H. Griefßer, J. Maucher, and V.V. Zyablov</i>	

Near Optimal Decoding for TCM Using the BIVA and Trellis Shaping	191
<i>Qi Wang, Lei Wei, and Rodney A. Kennedy</i>	

An Optimality Testing Algorithm for a Decoded Codeword of Binary Block Codes and Its Computational Complexity	201
<i>Yuansheng Tang, Tadao Kasami, and Toru Fujiwara</i>	

Algebra II

Recursive MDS-Codes and Pseudogeometries	211
<i>Elena Couselo, Santos Gonzalez, Victor Markov, and Alexandr Nechaev</i>	

Strength of MISTY1 without FL Function for Higher Order Differential Attack	221
<i>Hidema Tanaka, Kazuyuki Hisamatsu, and Toshinobu Kaneko</i>	

Code Construction

Quantum Reed–Solomon Codes	231
<i>Markus Grassl, Willi Geiselmann, and Thomas Beth</i>	

Capacity Bounds for the 3-Dimensional $(0, 1)$ Runlength Limited Channel	245
<i>Zsigmond Nagy and Kenneth Zeger</i>	

Rectangular Codes and Rectangular Algebra	252
<i>V. Sidorenko, J. Maucher, and M. Bossert</i>	

Codes and Algebra I: Algebraic Curves

Decoding Hermitian Codes with Sudan's Algorithm	260
<i>T. Høholdt and R. Refslund Nielsen</i>	
Computing a Basis of $\mathcal{L}(D)$ on an Affine Algebraic Curve with One Rational Place at Infinity	271
<i>Ryutaroh Matsumoto and Shinji Miura</i>	

Cryptography

Critical Noise for Convergence of Iterative Probabilistic Decoding with Belief Propagation in Cryptographic Applications	282
<i>Marc P.C. Fossorier, Miodrag J. Mihaljević, and Hideki Imai</i>	
An Authentication Scheme over Non-authentic Public Channel in Information-Theoretic Secret-Key Agreement	294
<i>Shengli Liu and Yumin Wang</i>	

Codes and Decoding

A Systolic Array Architecture for Fast Decoding of One-Point AG Codes and Scheduling of Parallel Processing on It	302
<i>Shojiro Sakata and Masazumi Kurihara</i>	

Convolutional Codes

Computing Weight Distributions of Convolutional Codes via Shift Register Synthesis	314
<i>Mehul Motani and Chris Heegard</i>	
Properties of Finite Response Input Sequences of Recursive Convolutional Codes	324
<i>Didier Le Ruyet, Hong Sun, and Han Vu Thien</i>	

Combinatorics III: Designs

Lower Bounds for Group Covering Designs	334
<i>K.K.P. Chanduka, Mahesh C. Bhandari, and Arbind K. Lal</i>	
Characteristic Functions of Relative Difference Sets, Correlated Sequences and Hadamard Matrices	346
<i>Garry Hughes</i>	

Decoding of Block Codes

Double Circulant Self-Dual Codes Using Finite-Field Wavelet Transforms	355
<i>F. Fekri, S.W. McLaughlin, R.M. Mersereau, and R.W. Schaffer</i>	

Algebra III: Rings and Fields

Linear Codes and Polylinear Recurrences over Finite Rings and Modules (a Survey)	365
<i>V.L. Kurakin, A.S. Kuzmin, V.T. Markov, A.V. Mikhalev, and A.A. Nechaev</i>	
Calculating Generators for Invariant Fields of Linear Algebraic Groups . . .	392
<i>Jörn Müller-Quade and Thomas Beth</i>	
Constructing Elements of Large Order in Finite Fields	404
<i>Joachim von zur Gathen and Igor Shparlinski</i>	

Modulation and Codes

New Lower Bounds on the Periodic Crosscorrelation of QAM Codes with Arbitrary Energy	410
<i>Serdar Boztas</i>	
Conjectures on the Size of Constellations Constructed from Direct Sums of PSK Kernels	420
<i>Matthew G. Parker</i>	

Codes and Algebra II: Gröbner Bases and AG Codes

A New Criterion for Normal Form Algorithms	430
<i>B. Mourrain</i>	
Discrete Fourier Transform and Gröbner Bases	444
<i>A. Poli, M.C. Gennero, and D. Xin</i>	

Block Codes II

On the State Complexities of Ternary Codes	454
<i>Sylvia Encheva and Gérard Cohen</i>	
Binary Optimal Linear Rate 1/2 Codes	462
<i>Koichi Betsumiya, T. Aaron Gulliver, and Masaaki Harada</i>	
On Binary/Ternary Error-Correcting Codes with Minimum Distance 4	472
<i>Patric R.J. Östergård</i>	

Algebra IV: Polynomials

The Euclidean Algorithm and Primitive Polynomials over Finite Fields . . .	482
<i>James W. Bond, Stefen Hui, and Hank Schmidt</i>	
On the Computational Hardness of Testing Square-Freeness of Sparse Polynomials	492
<i>Marek Karpinski and Igor Shparlinski</i>	
Mastrovito Multiplier for General Irreducible Polynomials	498
<i>A. Halbutoğulları and Ç.K. Koç</i>	
Author Index	509

Applied Algebra, Algebraic Algorithms and
Error-Correcting Codes

13th International Symposium, AAECC-13 Honolulu,
Hawaii, USA, November 15-19, 1999 Proceedings

Fossorier, M.; Imai, H.; Lin, S.; Poli, A. (Eds.)

1999, XIV, 518 p., Softcover

ISBN: 978-3-540-66723-0