Table of Contents

Invited Talks
Codes on Graphs: A Survey for Algebraists .......................... 1
  G. David Forney, Jr.

RA Codes Achieve AWGN Channel Capacity ......................... 10
  Hui Jin and Robert J. McEliece

Monomial Ideals and Planar Graphs ................................. 19
  Ezra Miller and Bernd Sturmfels

A Fast Program Generator of Fast Fourier Transforms ............ 29
  Michael Clausen and Meinard Müller

On Integer Programming Problems Related to Soft-Decision Iterative
Decoding Algorithms ............................................. 43
  Tadao Kasami

Curves with Many Points and Their Applications .................. 55
  Ian F. Blake

Codes and Iterative Decoding

New Sequences of Linear Time Erasure Codes Approaching the Channel
Capacity .......................................................... 65
  M. Amin Shokrollahi

On the Theory of Low-Density Convolutional Codes ................ 77
  Karin Engdahl,, Michael Lentmaier, and Kamil Sh. Zigangirov

Combinatorics I: Arithmetic

On the Distribution of Nonlinear Recursive Congruential Pseudorandom
Numbers of Higher Orders ........................................ 87
  Frances Griffin, Harald Niederreiter, and Igor E. Shparlinski

A New Representation of Boolean Functions ......................... 94
  Claude Carlet and Philippe Guillot

Combinatorics II: Graphs and Matrices

An Algorithm to Compute a Nearest Point in the Lattice \( A^*_n \) .......... 104
  I. Vaughan and L. Clarkson
# Table of Contents

**Sequences from Cocycles** ............................................ 121  
*Kathy J. Horadam*

## Block Codes I

On the Second Greedy Weight for Binary Linear Codes. ............ 131  
*Wende Chen and Torleiv Kløve*

On the Size of Identifying Codes .................................... 142  
*Uri Blass, Iiro Honkala, and Simon Litsyn*

## Algebra I: Rings and Fields

Fast Quantum Fourier Transforms for a Class of Non-abelian Groups .. 148  
*Markus Püschel, Martin Rötteler, and Thomas Beth*

Linear Codes and Rings of Matrices .............................. 160  
*M. Greferath and S.E. Schmidt*

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

## Decoding Methods

Some Results on Generalized Concatenation of Block Codes ....... 181  
*M. Bossert, H. Grießer, J. Maucher, and V.V. Zyablov*

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

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

## Algebra II

Recursive MDS-Codes and Pseudogeometries .......................... 211  
*Elena Couselo, Santos Gonzalez, Victor Markov, and Alexandr Nechaev*

Strength of MISTY1 without FL Function for Higher Order Differential Attack ........................................ 221  
*Hidema Tanaka, Kazuyuki Hisamatsu, and Toshinobu Kaneko*

## Code Construction

Quantum Reed–Solomon Codes ........................................... 231  
*Markus Grassl, Willi Geiselmann, and Thomas Beth*

Capacity Bounds for the 3-Dimensional $(0,1)$ Runlength Limited Channel .. 245  
*Zsízmond Nagy and Kenneth Zeger*
| Codes and Rectangular Algebra | V. Sidorenko, J. Maucher, and M. Bossert |
| Decoding Hermitian Codes with Sudan’s Algorithm | 260 |
| T. Høholdt and R. Refslund Nielsen |
| Computing a Basis of $L(D)$ on an Affine Algebraic Curve with One Rational Place at Infinity | 271 |
| Ryutaroh Matsumoto and Shinji Miura |
| Cryptography |
| Critical Noise for Convergence of Iterative Probabilistic Decoding with Belief Propagation in Cryptographic Applications | 282 |
| Marc P.C. Fossorier, Miodrag J. Mihaljević, and Hideki Imai |
| An Authentication Scheme over Non-authentic Public Channel in Information-Theoretic Secret-Key Agreement | 294 |
| Shengli Liu and Yumin Wang |
| Codes and Decoding |
| A Systolic Array Architecture for Fast Decoding of One-Point AG Codes and Scheduling of Parallel Processing on It | 302 |
| Shojiro Sakata and Masazumi Kurihara |
| Convolutional Codes |
| Computing Weight Distributions of Convolutional Codes via Shift Register Synthesis | 314 |
| Mehul Motani and Chris Heegard |
| Properties of Finite Response Input Sequences of Recursive Convolutional Codes | 324 |
| Didier Le Ruyet, Hong Sun, and Han Vu Thien |
| Combinatorics III: Designs |
| Lower Bounds for Group Covering Designs | 334 |
| K.K.P. Chanduka, Mahesh C. Bhandari, and Arbind K. Lal |
| Characteristic Functions of Relative Difference Sets, Correlated Sequences and Hadamard Matrices | 346 |
| Garry Hughes |
### Decoding of Block Codes

- **Double Circulant Self-Dual Codes Using Finite-Field Wavelet Transforms**
  - **F. Fekri, S.W. McLaughlin, R.M. Mersereau, and R.W. Schafer**
  - p. 355

### Algebra III: Rings and Fields

- **Linear Codes and Polynlinear Recurrences over Finite Rings and Modules (a Survey)**
  - **V.L. Kurakin, A.S. Kuzmin, V.T. Markov, A.V. Mikhalev, and A.A. Nechaev**
  - p. 365

- **Calculating Generators for Invariant Fields of Linear Algebraic Groups**
  - **Jörn Müller-Quade and Thomas Beth**
  - p. 392

- **Constructing Elements of Large Order in Finite Fields**
  - **Joachim von zur Gathen and Igor Shparlinski**
  - p. 404

### Modulation and Codes

- **New Lower Bounds on the Periodic Crosscorrelation of QAM Codes with Arbitrary Energy**
  - **Serdar Boztaş**
  - p. 410

- **Conjectures on the Size of Constellations Constructed from Direct Sums of PSK Kernels**
  - **Matthew G. Parker**
  - p. 420

### Codes and Algebra II: Gröbner Bases and AG Codes

- **A New Criterion for Normal Form Algorithms**
  - **B. Mourrain**
  - p. 430

- **Discrete Fourier Transform and Gröbner Bases**
  - **A. Poli, M.C. Gennaro, and D. Xin**
  - p. 444

### Block Codes II

- **On the State Complexities of Ternary Codes**
  - **Sylvia Encheva and Gérard Cohen**
  - p. 454

- **Binary Optimal Linear Rate 1/2 Codes**
  - **Koichi Betsumiya, T. Aaron Gulliver, and Masaaki Harada**
  - p. 462

- **On Binary/Ternary Error-Correcting Codes with Minimum Distance 4**
  - **Patric R.J. Östergård**
  - p. 472
## Algebra IV: Polynomials

The Euclidean Algorithm and Primitive Polynomials over Finite Fields . . . 482  
*James W. Bond, Stefen Hui, and Hank Schmidt*

On the Computational Hardness of Testing Square-Freeness of Sparse  
Polynomials .......................................................... 492  
*Marek Karpinski and Igor Shparlinski*

Mastrovito Multiplier for General Irreducible Polynomials ............... 498  
*A. Halbutoğulları and Ç. K. Koç*

**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