Table of Contents

Codes

The Order Bound for Toric Codes 1
Peter Beelen and Diego Ruano

An Extension of the Order Bound for AG Codes 11
Iwan Duursma and Radoslav Kirov

Sparse Numerical Semigroups 23
C. Munuera, F. Torres, and J. Villanueva

From the Euclidean Algorithm for Solving a Key Equation for Dual Reed–Solomon Codes to the Berlekamp-Massey Algorithm 32
Maria Bras-Amorós and Michael E. O'Sullivan

Rank for Some Families of Quaternary Reed-Muller Codes 43
Jaume Pernas, Jaume Pujol, and Mercè Villanueva

Optimal Bipartite Ramanujan Graphs from Balanced Incomplete Block Designs: Their Characterizations and Applications to Expander/LDPC Codes 53
Tom Høholdt and Heeralal Janwal

Simulation of the Sum-Product Algorithm Using Stratified Sampling 65
John Brevik, Michael E. O'Sullivan, Anya Umlauf, and Rich Wolski

A Systems Theory Approach to Periodically Time-Varying Convolutional Codes by Means of Their Invariant Equivalent 73
Joan-Josep Climent, Victoria Herranz, Carmen Perea, and Virtudes Tomás

On Elliptic Convolutional Goppa Codes 83
José Ignacio Iglesias Curto

The Minimum Hamming Distance of Cyclic Codes of Length $2p^s$ 92
Hakan Özadam and Ferruh Özbudak

There Are Not Non-obvious Cyclic Affine-invariant Codes 101
José Joaquín Bernal, Ángel del Río, and Juan Jacobo Simón

On Self-dual Codes over $\mathbf{Z_{16}}$ 107
Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada

Bibliografische Informationen
http://d-nb.info/994394535

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Cryptography

A Non-abelian Group Based on Block Upper Triangular Matrices with Cryptographic Applications 117
Rafael Álvarez, Leandro Tortosa, José Vicent, and Antonio Zamora

Word Oriented Cascade Jump σ–LFSR 127
Guang Zeng, Yang Yang, Wenbao Han, and Shuqin Fan

On Some Sequences of the Secret Pseudo-random Index j in RC4 Key Scheduling 137
Riddhipratim Basu, Subhamoy Maitra, Goutam Paul, and Tanmoy Talukdar

Very-Efficient Anonymous Password-Authenticated Key Exchange and Its Extensions 149
SeongHan Shin, Kazukuni Kobara, and Hideki Imai

Efficient Constructions of Deterministic Encryption from Hybrid Encryption and Code-Based PKE 159
Yang Cui, Kirill Morozov, Kazukuni Kobara, and Hideki Imai

Algebra

Noisy Interpolation of Multivariate Sparse Polynomials in Finite Fields 169
Álvar Ibeas and Arne Winterhof

New Commutative Semifields and Their Nuclei 179
Jürgen Bierbrauer

Spreads in Projective Hjelmslev Geometries 186
Ivan Landjev

On the Distribution of Nonlinear Congruential Pseudorandom Numbers of Higher Orders in Residue Rings 195
Edwin D. El-Mahassni and Domingo Gomez

Rooted Trees Searching for Cocyclic Hadamard Matrices over D_{4t} 204
Víctor Álvarez, José Ándrés Armario, María Dolores Frau, Félix Gudiel, and Amparo Osuna

Extended Abstracts

Interesting Examples on Maximal Irreducible Goppa Codes 215
Marta Giorgetti

Repeated Root Cyclic and Negacyclic Codes over Galois Rings..... 219
Sergio R. López-Permouth and Steve Szabo

Construction of Additive Reed-Muller Codes 223
J. Pujol, J. Rifà, and L. Ronquillo

Gröbner Representations of Binary Matroids 227
M. Borges-Quintana, M.A. Borges-Trenard, and E. Martínez-Moro

A Generalization of the Zig-Zag Graph Product by Means of the Sandwich Product 231
David M. Monarres and Michael E. O'Sullivan

Novel Efficient Certificateless Aggregate Signatures 235
Lei Zhang, Bo Qin, Qianhong Wu, and Futai Zhang

Bounds on the Number of Users for Random 2-Secure Codes 239
Manabu Hagiwara, Takahiro Yoshida, and Hideki Imai

Author Index 243