1. Record Nr. UNINA9910768478203321

Titolo	Applied Algebra, Algebraic Algorithms and Error-Correcting Codes : 14th International Symposium, AAECC-14, Melbourne, Australia, November 26-30, 2001. Proceedings / / edited by Serdar Boztas, Igor E. Shparlinski
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-45624-4
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (XII, 404 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2227
Disciplina	005.7/2
Soggetti	Algebra Coding theory Information theory Computer science—Mathematics Data encryption (Computer science) Algorithms Computer science - Mathematics Coding and Information Theory Symbolic and Algebraic Manipulation Cryptology Algorithm Analysis and Problem Complexity Computational Mathematics and Numerical Analysis Online resources.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Invited Contributions -- The Ubiquity of Reed-Muller Codes -- Self-dual Codes-Theme and Variations -- Design of Differential Space-Time Codes Using Group Theory -- Ideal Error-Correcting Codes: Unifying Algebraic and Number-Theoretic Algorithms -- Block Codes -- Self-dual Codes Using Image Restoration Techniques -- Low Complexity Tail-Biting Trellises of Self-dual codes of Length 24, 32 and 40 over GF

(2) and Z4 of Large Minimum Distance -- F q -Linear Cyclic Codes over F q m: DFT Characterization -- Code Constructions -- Cyclic Projective Reed-Muller Codes -- Codes Identifying Sets of Vertices -- Duality and Greedy Weights of Linear Codes and Projective Multisets -- Codes and Algebra:Rings and Fields -- Type II Codes over IF2r -- On Senary Simplex Codes -- Optimal Double Circulant Z4-Codes -- Constructions of Codes from Number Fields -- On Generalized Hamming Weights for Codes over Finite Chain Rings -- Information Rates and Weights of Codes in Structural Matrix Rings -- Codes and Algebra:Algebraic Geometry Codes -- On Hyperbolic Codes -- On Fast Interpolation Method for Guruswami-Sudan List Decoding of One-Point Algebraic-Geometry Codes -- Computing the Genus of a Class of Curves -- Sequences -- Iterations of Multivariate Polynomials and Discrepancy of Pseudorandom Numbers -- Even Length Binary Sequence Families with Low Negaperiodic Autocorrelation -- On the Non-existence of (Almost-)Perfect Quaternary Sequences -- Maximal Periods of x2 + c in Fq -- On the Aperiodic Correlation Function of Galois Ring m-Sequences -- Euclidean Modules and Multisequence Synthesis -- Cryptography -- On Homogeneous Bent Functions -- Partially Identifying Codes for Copyright Protection -- On the Generalised Hidden Number Problem and Bit Security of XTR -- CRYPTIM: Graphs as Tools for Symmetric Encryption -- Algorithms -- An Algorithm for Computing Cocyclic Matrices Developed over Some Semidirect Products -- Algorithms for Large Integer Matrix Problems -- On the Identification of Vertices and Edges Using Cycles -- Algorithms:Decoding -- On Algebraic Soft Decision Decoding of Cyclic Binary Codes -- Lifting Decoding Schemes over a Galois Ring -- Sufficient Conditions on Most Likely Local Sub-codewords in Recursive Maximum Likelihood Decoding Algorithms -- A Unifying System-Theoretic Framework for Errors-and-Erasures Reed-Solomon Decoding -- An Algorithm for Computing Rejection Probability of MLD with Threshold Test over BSC -- Algebraic Constructions -- Cartan’s Characters and Stairs of Characteristic Sets -- On the Invariants of the Quotients of the Jacobian of a Curve of Genus 2 -- Algebraic Constructions for PSK Space-Time Coded Modulation.

Sommario/riassunto

The AAECC Symposia Series was started in 1983 by Alain Poli (Toulouse), who, together with R. Desq, D. Lazard, and P. Camion, organized the ?rst conference. Originally the acronym AAECC meant “Applied Algebra and Error-Correcting Codes”. Over the years its meaning has shifted to “Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes”, re?ecting the growing importance of complexity in both decoding algorithms and computational algebra. AAECC aims to encourage cross-fertilization between algebraic methods and their applications in computing and communications. The algebraic orientation is towards ?nite ?elds, complexity, polynomials, and graphs. The applications orientation is towards both theoretical and practical error-correction coding, and, since AAECC 13 (Hawaii, 1999), towards cryptography. AAECC was the ?rst symposium with papers connecting Gr¨obner bases with E-C codes. The balance between theoretical and practical is intended to shift regularly; at AAECC-14 the focus was on the theoretical side. The main subjects covered were: – Codes: iterative decoding, decoding methods, block codes, code construction. – Codes and algebra: algebraic curves, Gr¨obner bases, and AG codes. – Algebra: rings and ?elds, polynomials. – Codes and combinatorics: graphs and matrices, designs, arithmetic. – Cryptography. – Computational algebra: algebraic algorithms. – Sequences for communications.