1. Record Nr. UNISA996465671803316

Titolo	Applied algebra, algebraic algorithms, and error-correcting codes : 13th international symposium, AAECC-13, Honolulu, Hawaii, USA, November 15-19, 1999 : proceedings / / Marc Fossorier [and three others], (editors)
Pubbl/distr/stampa	Berlin : , : Springer, , [1999] Â©1999
ISBN	3-540-46796-3
Edizione	[1st ed. 1999.]
Descrizione fisica	1 online resource (XIV, 518 p.)
Collana	Lecture notes in computer science ; ; 1719
Disciplina	005.72
Soggetti	Error-correcting codes (Information theory) Algebra - Data processing Algorithms
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 and index.
Nota di contenuto	Invited Papers -- Codes on Graphs: A Survey for Algebraists -- RA Codes Achieve AWGN Channel Capacity -- Monomial Ideals and Planar Graphs -- A Fast Program Generator of Fast Fourier Transforms -- On Integer Programming Problems Related to Soft-Decision Iterative Decoding Algorithms -- Curves with Many Points and Their Applications -- Codes and Iterative Decoding -- New Sequences of Linear Time Erasure Codes Approaching the Channel Capacity -- On the Theory of Low-Density Convolutional Codes -- Combinatorics I: Arithmetic -- On the Distribution of Nonlinear Recursive Congruential Pseudorandom Numbers of Higher Orders -- A New Representation of Boolean Functions -- Combinatorics II: Graphs and Matrices -- An Algorithm to Compute a Nearest Point in the Lattice A n * -- Sequences from Cocycles -- Block Codes I -- On the Second Greedy Weight for Binary Linear Codes -- On the Size of Identifying Codes -- Algebra I: Rings and Fields -- Fast Quantum Fourier Transforms for a Class of Non-abelian Groups -- Linear Codes and Rings of Matrices -- On ?4-Simplex Codes and Their Gray Images -- Decoding Methods -- Some Results on Generalized Concatenation of Block Codes -- Near

Optimal Decoding for TCM Using the BIVA and Trellis Shaping -- An Optimality Testing Algorithm for a Decoded Codeword of Binary Block Codes and Its Computational Complexity -- Algebra II -- Recursive MDS-Codes and Pseudogeometries -- Strength of ISTY1 without FL Function for Higher Order Differential Attack -- Code Construction -- Quantum Reed—Solomon Codes -- Capacity Bounds for the 3-Dimensional (0, 1) Runlength Limited Channel -- Rectangular Codes and Rectangular Algebra -- Codes and Algebra I: Algebraic Curves -- Decoding Hermitian Codes with Sudan's Algorithm -- Computing a Basis of on an affine algebraic curve with one rational place at infinit -- Cryptography -- Critical Noise for Convergence of Iterative Probabilistic Decoding with Belief Propagation in Cryptographic Applications -- An Authentication Scheme over Non-authentic Public Channel in Information-Theoretic Secret-Key Agreement -- Codes and Decoding -- A Systolic Array Architecture for Fast Decoding of One-Point AG Codes and Scheduling of Parallel Processing on It -- Convolutional Codes -- Computing Weight Distributions of Convolutional Codes Via Shift Register Synthesis -- Properties of Finite Response Input Sequences of Recursive Convolutional Codes -- Combinatorics III: Designs -- Lower Bounds for Group Covering Designs -- Characteristic Functions of Relative Difference Sets, Correlated Sequences and Hadamard Matrices -- Decoding of Block Codes -- Double Circulant Self-Dual Codes Using Finite-Field Wavelet Transforms -- Algebra III: Rings and Fields -- Linear Codes and Polylinear Recurrences over Finite Rings and Modules (A Survey) -- Calculating Generators for Invariant Fields of Linear Algebraic Groups -- Constructing Elements of Large Order in Finite Fields -- Modulation and Codes -- New Lower Bounds on the Periodic Crosscorrelation of QAM Codes with Arbitrary Energy -- Conjectures on the Size of Constellations Constructed from Direct Sums of PSK Kernels -- Codes and Algebra II: Gröbner Bases and AG Codes -- A New Criterion for Normal Form Algorithms -- Discrete Fourier Transform and Gröbner Bases -- Block Codes II -- On the State Complexities of Ternary Codes -- Binary Optimal Linear Rate 1/2 Codes -- On Binary/Ternary Error-Correcting Codes with Minimum Distance 4 -- Algebra IV: Polynomials -- The Euclidean Algorithm and Primitive Polynomials over Finite Fields -- On the Computational Hardness of Testing Square-Freeness of Sparse Polynomials -- Mastrovito Multiplier for General Irreducible Polynomials.

Sommario/riassunto

This book constitutes the refereed proceedings of the 19th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-13, held in Honolulu, Hawaii, USA in November 1999. The 42 revised full papers presented together with six invited survey papers were carefully reviewed and selected from a total of 86 submissions. The papers are organized in sections on codes and iterative decoding, arithmetic, graphs and matrices, block codes, rings and fields, decoding methods, code construction, algebraic curves, cryptography, codes and decoding, convolutional codes, designs, decoding of block codes, modulation and codes, Gröbner bases and AG codes, and polynomials.