Contents

Preface iii

Contributors ix

Conference Program xiii

Conference Participants xvii

I. FINITE FIELD THEORY

A Generalized Ore Transformation Applied to a Special Class of Polynomials over a Finite Field 3
Simon J. Agou

Polynomial Functions on Matrices over a Finite Field 15
Joel V. Brawley

Set-Complete Mappings on Finite Fields 33
Wun-Seng Chou

Primitive Elements and Polynomials: Existence Results 43
Stephen D. Cohen

Character Sums over Finite Fields 57
R. J. Evans

On Inversive Congruential Generators for Pseudorandom Numbers 75
Mary Flahive and Harald Niederreiter

A Special Class of Permutation Polynomials over Finite Fields 81
Javier Gomez-Calderon

Polynomial Factorizations and Character Sum Identities 87
John Greene

A Characterization of Some Minihypers and Codes Meeting the Griesmer Bound over $GF(q)$, $q > 9$ 105
N. Hamada and T. Helleseth

A New Family of Nonbinary Sequences with Large Linear Span 123
Chulki Kim and John J. Komo

Permutation Polynomials over Finite Fields 131
Gary L. Mullen

Recent Advances in the Theory of Finite Fields 153
Harald Niederreiter

On Nonexistence of Generalized Bent Functions 165
Dingyi Pei

Bent Permutations 173
Josef Pieprzyk

An Ideal Structure for Some Quasi-Cyclic Error-Correcting Codes 183
Roberta Evans Sabin

Periodicity Properties of kth Order Linear Recurrences with Irreducible Characteristic Polynomial over a Finite Field 195
Lawrence Somer

A p-adic Lifting Lemma and Its Applications to Permutation Polynomials 209
Daqing Wan

Algebraic Curves and Varieties over Finite Fields and Irreducible Cyclic Codes 217
J. Wolfmann

II. APPLICATIONS

Multiple Pulse Position Modulation with Generalized Constant Weight Codes 229
G. E. Atkin and K. Fung

Performance Analysis of Distributed Deadlock-Detection Algorithms 253
Omran Bukhres and Rajeev Moondhra

Suggestions for Quasi-Monte-Carlo Users 269
Henri Faure

Watchman Routes for a Pair of Convex Polygons 279
Laxmi P. Gewali and Rocky Lombardo

Block Source Coding over $GF(q)$ 291
J. D. Gibson and S. A. McClellan

On the Structural Complexity of Sequences, Images, and Automata 307
Ben Goertzel

Average Distance of Data Communicaton in Twisted Hypercubes 329
Kyung Hee Kwon, Shahram Latifi, and Si-Qing Zheng

Linear Algebraic Structures of Algorithmic Mappings on Array Processors 341
George Miel

Finite Fields and Cryptology 359
Harald Niederreiter

Finite Fields, Pseudorandom Numbers, and Quasirandom Points 375
Harald Niederreiter

An Application of Finite Field Theory to Computerized Tomography:
A Spatial Limited Angle Model 395
Pablo M. Salzberg

Tree Coding and IFS Fractals 403
Matthew Varghese and Seshadri Mohan

Cryptography Using Complementing Subsets of Polynomials
over Finite Fields 411
William A. Webb

An Image Compression Algorithm and Its Implementation 417
E. A. Yfantis, S. Baker, and G. M. Gallitano

III. OPEN PROBLEMS AND CONJECTURES 429

Josef Pieprzyk, Andrew Klapper, Daqing Wan, Thomas Hansen and
Gary L. Mullen, H. Niederreiter, Stephen D. Cohen, Gary L. Mullen
and Harald Niederreiter, J. F. Dillon

Index 439