



Handbook of Finite Fields

Hardback \$139.95 ISBN 9781439873786

Cat# K13417

Series:

Discrete Mathematics and Its Applications

Published:

June 17, 2013 by Chapman and Hall/CRC

Content:

1068 Pages | 12 Illustrations

Author(s):

Gary L. Mullen; Daniel Panario

Table of Contents

Introduction

History of Finite Fields, *Roderick Gow*

Finite fields in the 18th and 19th centuries

Introduction to Finite Fields

Basic properties of finite fields, *Gary L. Mullen and Daniel Panario*

Tables, *David Thomson*

Theoretical Properties

Irreducible Polynomials

Counting irreducible polynomials, *Joseph L. Yucas*

Construction of irreducible, *Melsik Kyuregyan*

Conditions for reducible polynomials, *Daniel Panario*

Weights of irreducible polynomials, *Omran Ahmadi*

Prescribed coefficients, *Stephen D. Cohen*

Multivariate polynomials, *Xiang-dong Hou*

Primitive Polynomials

Introduction to primitive polynomials, *Gary L. Mullen and Daniel Panario*

Prescribed coefficients, *Stephen D. Cohen*

Weights of primitive polynomials, *Stephen D. Cohen*
Elements of high order, *José Felipe Voloch*

Bases

Duality theory of bases, *Dieter Jungnickel*
Normal bases, *Shuhong Gao and Qunying Liao*
Complexity of normal bases, *Shuhong Gao and David Thomson*
Completely normal bases, *Dirk Hachenberger*

Exponential and Character Sums

Gauss, Jacobi, and Kloosterman sums, *Ronald J. Evans*
More general exponential and character sums, *Antonio Rojas-León*
Some applications of character sums, *Alina Ostafe and Arne Winterhof*
Sum-product theorems and applications, *Moubariz Z. Garaev*

Equations over Finite Fields

General forms, *Daqing Wan*
Quadratic forms, *Robert Fitzgerald*
Diagonal equations, *Francis Castro and Ivelisse Rubio*

Permutation Polynomials

One variable, *Gary L. Mullen and Qiang Wang*
Several variables, *Rudolf Lidl and Gary L. Mullen*
Value sets of polynomials, *Gary L. Mullen and Michael E. Zieve*
Exceptional polynomials, *Michael E. Zieve*

Special Functions over Finite Fields

Boolean functions, *Claude Carlet*
PN and APN functions, *Pascale Charpin*
Bent and related functions, *Alexander Kholosha and Alexander Pott*
 k -polynomials and related algebraic objects, *Robert Coulter*
Planar functions and commutative semifields, *Robert Coulter*
Dickson polynomials, *Qiang Wang and Joseph L. Yucas*
Schur's conjecture and exceptional covers, *Michael D. Fried*

Sequences over Finite Fields

Finite field transforms, *Gary McGuire*
LFSR sequences and maximal period sequences, *Harald Niederreiter*
Correlation and autocorrelation of sequences, *Tor Helleseth*
Linear complexity of sequences and multisequences, *Wilfried Meidl and Arne Winterhof*
Algebraic dynamical systems over finite fields, *Igor Shparlinski*

Algorithms

Computational techniques, *Christophe Doche*
Univariate polynomial counting and algorithms, *Daniel Panario*
Algorithms for irreducibility testing and for constructing irreducible polynomials, *Mark Giesbrecht*
Factorization of univariate polynomials, *Joachim von zur Gathen*
Factorization of multivariate polynomials, *Erich Kaltofen and Grégoire Lecerf*
Discrete logarithms over finite fields, *Andrew Odlyzko*
Standard models for finite fields, *Bart de Smit and Hendrik Lenstra*

Curves over Finite Fields

Introduction to function fields and curves, *Arnaldo Garcia and Henning Stichtenoth*
Elliptic curves, *Joseph Silverman*
Addition formulas for elliptic curves, *Daniel J. Bernstein and Tanja Lange*

Hyperelliptic curves, *Michael John Jacobson, Jr. and Renate Scheidler*
Rational points on curves, *Arnaldo Garcia and Henning Stichtenoth*
Towers, *Arnaldo Garcia and Henning Stichtenoth*
Zeta functions and L-functions, *Lei Fu*
 p -adic estimates of zeta functions and L-functions, *Régis Blache*
Computing the number of rational points and zeta functions, *Daqing Wan*

Miscellaneous Theoretical Topics

Relations between integers and polynomials over finite fields, *Gove Effinger*
Matrices over finite fields, *Dieter Jungnickel*
Classical groups over finite fields, *Zhe-Xian Wan*
Computational linear algebra over finite fields, *Jean-Guillaume Dumas and Clément Pernet*
Carlitz and Drinfeld modules, *David Goss*

Applications

Combinatorial

Latin squares, *Gary L. Mullen*
Lacunary polynomials over finite fields, *Simeon Ball and Aart Blokhuis*
Affine and projective planes, *Gary Ebert and Leo Storme*
Projective spaces, *James W.P. Hirschfeld and Joseph A. Thas*
Block designs, *Charles J. Colbourn and Jeffrey H. Dinitz*
Difference sets, *Alexander Pott*
Other combinatorial structures, *Jeffrey H. Dinitz and Charles J. Colbourn*
 (t, m, s) -nets and (t, s) -sequences, *Harald Niederreiter*
Applications and weights of multiples of primitive and other polynomials, *Brett Stevens*
Ramanujan and expander graphs, *M. Ram Murty and Sebastian M. Cioaba*

Algebraic Coding Theory

Basic coding properties and bounds, *Ian Blake and W. Cary Huffman*
Algebraic-geometry codes, *Harald Niederreiter*
LDPC and Gallager codes over finite fields, *Ian Blake and W. Cary Huffman*
Turbo codes over finite fields, *Oscar Takeshita*
Raptor codes, *Ian Blake and W. Cary Huffman*
Polar codes, *Simon Litsyn*

Cryptography

Introduction to cryptography, *Alfred Menezes*
Stream and block ciphers, *Guang Gong and Kishan Chand Gupta*
Multivariate cryptographic systems, *Jintai Ding*
Elliptic curve cryptographic systems, *Andreas Enge*
Hyperelliptic curve cryptographic systems, *Nicolas Thériault*
Cryptosystems arising from Abelian varieties, *Kumar Murty*
Binary extension field arithmetic for hardware implementations, *M. Anwarul Hasan and Haining Fan*

Miscellaneous Applications

Finite fields in biology, *Franziska Hinkelmann and Reinhard Laubenbacher*
Finite fields in quantum information theory, *Martin Roetteler and Arne Winterhof*
Finite fields in engineering, *Jonathan Jedwab and Kai-Uwe Schmidt*

Bibliography

Index

