Contents

Preface vii

Chapter 5. Curves with Many Points. I: Modular Curves 1
  5.1. Classical Modular Curves 2
    5.1.1. Modular Curves 2
    5.1.2. Modular Curves over Finite Fields 12
    5.1.3. Codes 16
  5.2. Drinfeld Modular Curves 21
    5.2.1. Elliptic Modules 22
    5.2.2. Drinfeld Curves 24
    5.2.3. Codes 33
  5.3. Elkies Explicit Towers 37
    5.3.1. Classical Modular Curve Towers 37
    5.3.2. Explicit Towers of Drinfeld Modular Curves 42
Historical and Bibliographic Notes 47

Chapter 6. Class Field Theory 49
  6.1. Global Fields 49
    6.1.1. Function Fields 50
    6.1.2. Number Fields 55
  6.2. Local Class Field Theory 62
  6.3. Global Class Field Theory 68
    6.3.1. Artin Map 68
    6.3.2. Main Theorems 71
    6.3.3. Explicit Class Field Theory for Function Fields 74
  6.4. Class Field Towers 79
    6.4.1. Class Field Tower Problem 79
    6.4.2. Applications to $A(q)$ 81
Historical and Bibliographic Notes 85

Chapter 7. Curves with Many Points. II 87
  7.1. Oesterlé Bound 88
  7.2. Deligne–Lusztig Curves 94
    7.2.1. Group Codes on Hermitian Curves 94
    7.2.2. Suzuki Curves 96
    7.2.3. Ree Curves 101
    7.2.4. Deligne–Lusztig Curves via Class Field Theory 104
7.3. Some Curves of Small Genera 107
   7.3.1. Curves with Many Points from Ray Class Fields 107
   7.3.2. Fibre Products 111
   7.3.3. Maximal Curves Covered by a Hermitian Curve 114
7.4. Recursive Towers 116
   7.4.1. Some Basic Facts on Towers 116
   7.4.2. Some Specific García–Stichtenoth Towers and the
           Elkies Conjecture 120
   7.4.3. Polynomials Constructible Codes from the $W_1$ Tower 125
   7.4.4. A Very Good Tower for $q = p^{2m+1}$, $m \geq 1$ 128
   7.4.5. Good Recursive Towers over $\mathbb{F}_q$, $q \geq 4$ 130
7.5. Two Nonstandard Problems 133
   7.5.1. Curves with a Prescribed Number of Points 133
   7.5.2. Curves for Every Genus 135
Historical and Bibliographic Notes 138

Chapter 8. Infinite Global Fields 141
8.1. Invariants and Basic Inequalities 141
   8.1.1. Invariants of Infinite Global Fields 146
   8.1.2. Basic Inequalities 149
   8.1.3. Limit Zeta Function 155
   8.1.4. Limit Explicit Formula 158
8.2. The Generalized Brauer–Siegel Theorem 163
   8.2.1. Main Result 163
   8.2.2. Bounds for the Brauer–Siegel Ratios 171
8.3. Class Field Tower Examples 175
   8.3.1. Unramified Towers with Splitting Conditions 175
   8.3.2. Hajir–Maire Tame Towers 183
8.4. Further Theory and Open Questions 185
   8.4.1. Common Questions 185
   8.4.2. Results Specific for the Function Field Case and
           Corresponding Problems 188
Historical and Bibliographic Notes 192

Chapter 9. Decoding: Some Examples 195
9.1. List Decoding 195
   9.1.1. Johnson Bound 196
   9.1.2. Capacity of List Decoding 198
9.2. Guruswami–Sudan Algorithm 200
   9.2.1. Decoding of Reed–Solomon Codes 200
   9.2.2. Decoding of Algebraic Geometry Codes 203
   9.2.3. Representations of Algebraic Geometry Codes 207
9.3. Example: Hermitian Curves 211
   9.3.1. Bases and Interpolation 211
   9.3.2. Factorization 214
CONTENTS

9.4. Approaching the Singleton Bound
  9.4.1. Periodic Affine Subspaces
  9.4.2. Subspace Designs
  9.4.3. Case of the General Algebraic Geometry Codes
  9.4.4. Codes from the $\mathcal{W}_1$ Tower

Historical and Bibliographic Notes

Chapter 10. Sphere Packings
  10.1. Definitions, Examples, and Constructions
    10.1.1. Parameters and Some Basic Examples
    10.1.2. Asymptotic Problems
    10.1.3. Random Packings
  10.2. Asymptotically Dense Packings
    10.2.1. Constructions of Dense Packings
    10.2.2. Spherical Codes and Kissing Numbers
    10.2.3. Lattices with Exponentially Large Kissing Numbers
  10.3. Lattices from Global Fields
    10.3.1. Additive Constructions
    10.3.2. Multiplicative Constructions
    10.3.3. Congruence Constructions
  10.4. Mordell–Weil Lattices
    10.4.1. Shioda Lattices
    10.4.2. Elkies Lattices

Appendix: Parameters of Some Packings

Historical and Bibliographic Notes

Chapter 11. Codes from Multidimensional Varieties
  11.1. Complete Intersections and Reed–Muller Codes
    11.1.1. Tsfasman–Serre–Sørensen Bound
    11.1.2. Generalization to Several Polynomials: Tsfasman–Boguslavsky Conjecture
    11.1.3. Reed–Muller Codes and the Affine Case
  11.2. General Algebraic Sets
    11.2.1. Lachaud’s Bounds
    11.2.2. Couvreur’s Bound
  11.3. Codes on Surfaces
    11.3.1. Some Elements of the Theory of Surfaces
    11.3.2. Cubic Surfaces over a Finite Field
    11.3.3. Rational Surfaces for Good Codes
  11.4. Hermitian Varieties and Quadrics
    11.4.1. Hermitian Varieties
    11.4.2. Quadrics
  11.5. Grassmann and Schubert Codes
    11.5.1. Grassmann Codes
    11.5.2. Schubert Codes
11.6. Codes from Flag Varieties 328
11.6.1. Flag Varieties 328
11.6.2. Examples 329
11.6.3. Two More Examples 331
Historical and Bibliographic Notes 333

Chapter 12. Applications 335
12.1. Fast Multiplication in Finite Fields 335
12.1.1. Tensor Rank and Bilinear Complexity 335
12.1.2. The Extended Chudnovsky Algorithm 338
12.2. Cryptographic Applications 343
12.2.1. Authentication Codes from Algebraic Curves 343
12.2.2. Arithmetic Secret Sharing Schemes 350
12.3. Quantum Codes 357
12.3.1. Quantum Error-Correcting Codes 357
12.3.2. Quantum Codes from Algebraic Geometry Codes 360
12.3.3. Nonbinary Case 366
12.4. Niederreiter–Rosenbloom–Tsfasman Metric 369
12.4.1. NRT Metric Spaces: Definitions and Bounds 369
12.4.2. Examples and Asymptotic Bounds 372
12.4.3. Uniform Nets and Sequences 378
12.5. Locally Recoverable Codes 384
12.5.1. Optimal LRC Codes 384
12.5.2. Locally Recoverable Codes on Algebraic Curves 386
12.5.3. Asymptotic Behaviour 389
Historical and Bibliographic Notes 395

Some Basic Facts from Volume 1 397
A.1. Codes and Projective Systems 397
A.1.1. Codes and Their Parameters 397
A.1.2. \([n,k,d]_q\) Systems 398
A.1.3. Bounds 399
A.1.4. Asymptotic Problems 400
A.1.5. Some Code Constructions and Their Parameters 401
A.2. Curves over Finite Fields 402
A.2.1. Algebraic Curves 402
A.2.2. Algebraic Function Fields 405
A.2.3. Finite Field Case 407
A.3. Algebraic Geometry Codes 412
A.3.1. Constructions and Their Parameters 412
A.3.2. Example: Hermitian Curves and Codes 412
A.3.3. Asymptotic Results 414

Bibliography 417
List of Names 437
Index 441