Contents

Preface xxiii

Acknowledgments xxiv

About the author xxvi

I An elementary introduction to coding 1

1 The concept of coding 3
- 1.1 Bitstrings and binary operations . . . 3
- 1.2 The Hamming distance . . . 7
- 1.3 Binary codes . . . 9
- 1.4 Error-correcting codes in general . . . 12
- 1.5 The binary symmetric channel . . . 14
- 1.6 The sphere-packing bound . . . 19

2 Binary linear codes 23
- 2.1 The concept of binary linear codes . . . 23
- 2.2 Block coding . . . 27
- 2.3 The effect of coding . . . 29
- 2.4 Duality . . . 30
- 2.5 Binary Hamming and Simplex codes . . . 33
- 2.6 Principle of duality . . . 37

3 General linear codes 41
- 3.1 Prime fields . . . 41
- 3.2 Finite fields . . . 43
- 3.3 Linear codes over finite fields . . . 47
- 3.4 Duality and orthogonal arrays . . . 50
- 3.5 Weight distribution . . . 58
- 3.6 The game of SET . . . 63
- 3.7 Syndrome decoding . . . 66

4 Singleton bound and Reed-Solomon codes 71

5 Recursive constructions I 81
- 5.1 Shortening and puncturing . . . 81
- 5.2 Concatenation . . . 87

Bierbrauer, Jürgen
Introduction to coding theory

digitalisiert durch:
IDS Basel Bern

6 Universal hashing 93

7 Designs and the binary Golay code 97

8 Shannon entropy 101

9 Asymptotic results 113

10 Three-dimensional codes, projective planes 125

11 Summary and outlook 131

II Theory and applications of codes 133

12 Subfield codes and trace codes 135
- 12.1 The trace 135
- 12.2 Trace codes and subfield codes 140
- 12.3 Galois closed codes 143
- 12.4 Automorphism groups 146

13 Cyclic codes 151
- 13.1 Some primitive cyclic codes of length 15 151
- 13.2 Theory of cyclic codes 154
- 13.3 Decoding BCH codes 170
- 13.4 Constacyclic codes 182
- 13.5 Remarks 186

14 Recursive constructions, covering radius 189
- 14.1 Construction X 189
- 14.2 Covering radius 198

15 The linear programming method 205
- 15.1 Introduction to linear programming 205
- 15.2 The Fourier transform 221
- 15.3 Some explicit LP bounds 230
- 15.4 The bound of four 232

16 OA in statistics and computer science 239
- 16.1 OA and independent random variables 239
- 16.2 Linear shift register sequences 242
- 16.3 Cryptography and S boxes 250
- 16.4 Two-point-based sampling 254
- 16.5 Resilient functions 256
- 16.6 Derandomization of algorithms 265
- 16.7 Authentication and universal hashing 270

17 The geometric description of linear codes 285
17.1 Linear codes as sets of points 285
17.2 Quadratic forms, bilinear forms and caps 312
17.3 Caps: Constructions and bounds 332

18 Additive codes and network codes 349
18.1 Basic constructions and applications 349
18.2 The cyclic theory of additive codes 360
18.2.1 Code equivalence and cyclicity 360
18.2.2 The linear case $m = 1$ 370
18.3 Additive quaternary codes: The geometric approach 373
18.4 Quantum codes 380
18.5 Network codes and subspace codes 389

III Codes and algebraic curves 395

19 Introduction 397
19.1 Polynomial equations and function fields 397
19.2 Places of the rational function field 401

20 Function fields, their places and valuations 405
20.1 General facts 405
20.2 Divisors and the genus 409
20.3 The Riemann-Roch theorem 414
20.4 Some hyperelliptic equations 417

21 Determining the genus 421
21.1 Algebraic extensions of function fields 421
21.2 The hyperelliptic case 423
21.3 The Kloosterman codes and curves 424
21.4 Subrings and integrality 426
21.5 The Riemann-Hurwitz formula 427

22 AG codes, Weierstraß points and universal hashing 431
22.1 The basic construction 431
22.2 Pole orders 432
22.3 Examples of function fields and projective equations 433
22.4 The automorphism group 440
22.5 AG codes and universal hashing 443
22.6 The Hasse-Weil bound 444

23 The last chapter 447
23.1 List decoding 447
23.2 Expander codes 450
23.3 tms-nets 452
23.4 Sphere packings 456

23.5 Permutation codes 466
23.6 Designs 468
23.7 Nonlinear codes 470
23.8 Some highly symmetric codes 479
23.9 Small fields 482
23.10 Short codes 483

References **487**

Index **503**