Preface

Preface to the third printing

Contents

Linear codes

Linear codes

Properties of a linear code

At the receiving end

More about decoding a linear code

Error probability

Shannon's theorem on the existence of good codes

Hamming codes

The dual code

Construction of new codes from old (II)

Some general properties of a linear code

Summary of Chapter 1

Notes on Chapter 1

Nonlinear codes, Hadamard matrices, designs and the Golay code

Nonlinear codes

The Plotkin bound

Hadamard matrices and Hadamard codes

Conferences matrices

t-designs

An introduction to the binary Golay code

The Steiner system S(5, 6, 12), and nonlinear single-error correcting codes

An introduction to the Nordstrom-Robinson code

Construction of new codes from old (III)

Notes on Chapter 2

An introduction to BCH codes and finite fields

Double-error-correcting BCH codes (I)

Construction of the field GF(16)

Double-error-correcting BCH codes (II)

Computing in a finite field

Notes on Chapter 3

Finite fields

Introduction

Finite fields: the basic theory

Minimal polynomials

How to find irreducible polynomials

Tables of small fields

The automorphism group of GF(p[superscript m])
The automorphism group of a code p. 229
The Mattson-Solomon polynomial p. 239
Some weight distributions p. 251
Notes on Chapter 8 p. 255
BCH codes
   Introduction p. 257
   The true minimum distance of a BCH code p. 259
   The number of information symbols in BCH codes p. 262
   A table of BCH codes p. 266
   Long BCH codes are bad p. 269
   Decoding BCH codes p. 270
   Quadratic equations over $\text{GF}(2^{[\text{superscript m}]})$ p. 277
   Double-error-correcting BCH codes are quasi-perfect p. 279
   The Carlitz-Uchiyama bound p. 280
   Some weight distributions are asymptotically normal p. 282
   Notes on Chapter 9 p. 291
Reed-Solomon and Justesen codes
   Introduction p. 294
   Reed-Solomon codes p. 294
   Extended RS codes p. 296
   Idempotents of RS codes p. 296
   Mapping $\text{GF}(2^{[\text{superscript m}]})$ codes into binary codes p. 298
   Burst error correction p. 301
   Encoding Reed-Solomon codes p. 301
   Generalized Reed-Solomon codes p. 303
   Redundant residue codes p. 305
   Decoding RS codes p. 306
   Justesen codes and concatenated codes p. 306
   Notes on Chapter 10 p. 315
MDS codes
   Introduction p. 317
   Generator and parity check matrices p. 318
   The weight distribution of an MDS code p. 319
   Matrices with every square submatrix nonsingular p. 321
   MDS codes from RS codes p. 323
   n-arcs p. 326
   The known results p. 327
   Orthogonal arrays p. 328
   Notes on Chapter 11 p. 329
Alternant, Goppa and other generalized BCH codes
Introduction

Alternant codes

Goppa codes

Further properties of Goppa codes

Extended double-error-correcting Goppa codes are cyclic

Generalized Srivastava codes

Chien-Choy generalized BCH codes

The Euclidean algorithm

Decoding alternant codes

Notes on Chapter 12

Reed-Muller codes

Introduction

Boolean functions

Reed-Muller Codes

RM codes and geometries

The minimum weight vectors generate the code

Encoding and decoding (I)

Encoding and decoding (II)

Other geometrical codes

Automorphism groups of the RM codes

Mattson-Solomon polynomials of RM codes

The action of the general affine group on Mattson-Solomon polynomials

Notes on Chapter 13

First-order Reed-Muller codes

Introduction

Pseudo-noise sequences

Cosets of the first-order Reed-Muller code

Encoding and decoding R(1, m)

Bent functions

Notes on Chapter 14

Second-order Reed-Muller, Kerdock and Preparata codes

Introduction

Weight distribution of second-order Reed-Muller codes

Weight distribution of arbitrary Reed-Muller codes

Subcodes of dimension 2m of R(2, m)* and R(2, m)

The Kerdock code and generalizations

The Preparata code

Goethals’ generalization of the Preparata codes

Notes on Chapter 15

Quadratic-residue codes
<table>
<thead>
<tr>
<th>Notes on Chapter 18</th>
<th>p. 594</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-dual codes and invariant theory</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>p. 596</td>
</tr>
<tr>
<td>An introduction to invariant theory</td>
<td>p. 598</td>
</tr>
<tr>
<td>The basic theorems of invariant theory</td>
<td>p. 607</td>
</tr>
<tr>
<td>Generalizations of Gleason's theorems</td>
<td>p. 617</td>
</tr>
<tr>
<td>The nonexistence of certain very good codes</td>
<td>p. 624</td>
</tr>
<tr>
<td>Good self-dual codes exist</td>
<td>p. 629</td>
</tr>
<tr>
<td>Notes on Chapter 19</td>
<td>p. 633</td>
</tr>
<tr>
<td>The Golay codes</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>p. 634</td>
</tr>
<tr>
<td>The Mathieu group $M_{24}$</td>
<td>p. 636</td>
</tr>
<tr>
<td>$M_{24}$ is five-fold transitive</td>
<td>p. 637</td>
</tr>
<tr>
<td>The order of $M_{24}$ is $24.23.22.21.20.48$</td>
<td>p. 638</td>
</tr>
<tr>
<td>The Steiner system $S(5, 8, 24)$ is unique</td>
<td>p. 641</td>
</tr>
<tr>
<td>The Golay codes $g_{23}$ and $g_{24}$ are unique</td>
<td>p. 646</td>
</tr>
<tr>
<td>The automorphism groups of the ternary Golay codes</td>
<td>p. 647</td>
</tr>
<tr>
<td>The Golay codes $g_{11}$ and $g_{12}$ are unique</td>
<td>p. 648</td>
</tr>
<tr>
<td>Notes on Chapter 20</td>
<td>p. 649</td>
</tr>
<tr>
<td>Association schemes</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>p. 651</td>
</tr>
<tr>
<td>Association schemes</td>
<td>p. 651</td>
</tr>
<tr>
<td>The Hamming association scheme</td>
<td>p. 656</td>
</tr>
<tr>
<td>Metric schemes</td>
<td>p. 659</td>
</tr>
<tr>
<td>Symplectic forms</td>
<td>p. 661</td>
</tr>
<tr>
<td>The Johnson scheme</td>
<td>p. 665</td>
</tr>
<tr>
<td>Subsets of association schemes</td>
<td>p. 666</td>
</tr>
<tr>
<td>Subsets of symplectic forms</td>
<td>p. 667</td>
</tr>
<tr>
<td>$t$-designs and orthogonal arrays</td>
<td>p. 670</td>
</tr>
<tr>
<td>Notes on Chapter 21</td>
<td>p. 671</td>
</tr>
<tr>
<td>Tables of the best codes known</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>p. 673</td>
</tr>
<tr>
<td>Figure 1, a small table of $A(n, d)$</td>
<td>p. 683</td>
</tr>
<tr>
<td>Figure 2, an extended table of the best codes known</td>
<td>p. 690</td>
</tr>
<tr>
<td>Figure 3, a table of $A(n, d, w)$</td>
<td>p. 691</td>
</tr>
<tr>
<td>Finite geometries</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>p. 692</td>
</tr>
<tr>
<td>Finite geometries, $PG(m, q)$ and $EG(m, q)$</td>
<td>p. 692</td>
</tr>
<tr>
<td>Properties of $PG(m, q)$ and $EG(m, q)$</td>
<td>p. 697</td>
</tr>
<tr>
<td>Projective and affine planes</td>
<td>p. 701</td>
</tr>
</tbody>
</table>
Notes on Appendix B  p. 702
Bibliography  p. 703
Index  p. 757

*Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.*