

Contents

PREFACE	ix
ACKNOWLEDGMENTS	xi
1. Finite Fields and Coding Theory	
1.1 Introduction	1
1.2 Fields, Extensions, and Polynomials	2
1.3 Fundamental Properties of Finite Fields	7
1.4 Vector Spaces over Finite Fields	10
1.5 Linear Codes	15
1.6 Polynomials over Finite Fields	29
1.7 Cyclic Codes	40
1.8 Linear Transformations of Vector Spaces over Finite Fields	58
1.9 Code Invariance under Permutation Groups	63
1.10 The Polynomial Approach to Coding	66
1.11 Bounds on Code Dictionaries	83
1.12 Comments	89
Exercises	90
2. Combinatorial Constructions and Coding	
2.1 Introduction	95
2.2 Finite Geometries: Their Collineation Groups and Codes	95
2.3 Balanced Incomplete Block Designs and Codes	119
2.4 Latin Squares and Steiner Triple Systems	132
2.5 Quadratic Residues and Codes	139

2.6	Hadamard Matrices, Difference Sets, and Their Codes	144
2.7	Self-Dual and Quasicyclic Codes	152
2.8	Perfect Codes	161
2.9	Comments	165
	Exercises	166

3. Coding and Combinatorics

3.1	Introduction	170
3.2	General t Designs	170
3.3	Matroids	173
3.4	Chains and Chain Groups	175
3.5	Dual Chain Groups	178
3.6	Matroids, Graphs, and Coding	179
3.7	Perfect Codes and t Designs	183
3.8	Nearly Perfect Codes and t Designs	186
3.9	Balanced Codes and t Designs	189
3.10	Equidistant Codes	192
3.11	Comments	201
	Exercises	201

4. The Structure of Semisimple Rings

4.1	Introduction	204
4.2	Rings, Ideals, and the Minimum Condition	205
4.3	Nilpotent Ideals and the Radical	207
4.4	The Structure of Semisimple Rings	210
4.5	The Structure of Simple Rings	215
4.6	The Group Algebra and Group Characters	217
4.7	The Structure of Cyclic Codes	222
4.8	Abelian Codes	227
4.9	Comments	244
	Exercises	244

5. Group Representations

5.1	Introduction	246
5.2	Representation of Groups	246
5.3	Group Characters	253
5.4	Orthogonality Relationships and Properties of Group Characters	259
5.5	Subduced and Induced Representations	269
5.6	Direct and Semidirect Products	273
5.7	Real Representations	276
5.8	Modules, Group Algebras, and Representations	284
5.9	Comments	290
	Exercises	290

6. Group Codes for the Gaussian Channel

6.1	Introduction	292
6.2	Codes for the Gaussian Channel	293
6.3	Group Codes for the Gaussian Channel	297
6.4	The Configuration Matrix	304
6.5	Distance Properties of Group Codes	314
6.6	The Initial Vector Problem	318
6.7	Comments	326
	Exercises	326

Appendix A.	The Möbius Inversion Formula	329
--------------------	-------------------------------------	------------

Appendix B.	Lucas's Theorem	330
--------------------	------------------------	------------

Appendix C.	The Mathieu Groups	331
--------------------	---------------------------	------------

References	339
-------------------	------------

INDEX	349
--------------	------------