Table of Contents

Preface ..... **V**

Table of Contents ..... **XI**

List of Tables ..... **XV**

List of Figures ..... **XIX**

List of Symbols ..... **XXI**

1 Linear Codes

1.1 Introduction **3**
1.2 Linear Codes, Encoding and Decoding **11**
1.3 Check Matrices and the Dual Code **20**
1.4 Classification by Isometry **28**
1.5 Semilinear Isometry Classes of Linear Codes **41**
1.6 The Weight Enumerator **51**
1.7 Systematic Encoding, Information Sets **65**
1.8 A Minimum Distance Algorithm **70**

2 Bounds and Modifications

2.1 Combinatorial Bounds for the Parameters **82**
2.2 New Codes from Old and the Minimum Distance **94**
2.3 Further Modifications and Constructions **102**
2.4 Reed–Muller-Codes **118**
2.5 MDS-Codes **128**

3 Finite Fields

3.1 Finite Fields – An Introduction **139**
3.2 Existence and Uniqueness of Finite Fields **149**
3.3 The Galois Group and Normal Bases **167**
3.4 Enumeration under Group Actions, Lyndon Words **170**
3.5 Construction of Irreducible Polynomials **182**
3.6 Representations of Field Elements **203**
3.7 Projective Geometry **205**

4 Cyclic Codes

4.1 Cyclic Codes as Group Algebra Codes **214**
4.2 Polynomial Representation of Cyclic Codes **220**
4.3 BCH-Codes and Reed–Solomon-Codes **237**
4.4 Quadratic-Residue-Codes, Golay-Codes **252**

4.5	Idempotents and the Discrete Fourier Transform	**268**
4.6	Alternant-Codes, Goppa-Codes	**285**
4.7	The Structure Theorem	**292**
4.8	Codes of p-Power Block Length	**311**
4.9	Bounds for the Minimum Distance	**319**
4.10	Reed–Muller-Codes	**327**
4.11	Encoding	**334**
4.12	Permutation Decoding	**338**
4.13	Error-Correcting Pairs	**346**
4.14	Majority Logic Decoding	**350**
5	**Mathematics and Audio Compact Discs**	
5.1	Fourier Transform, Shannon's Sampling Theorem	**370**
5.2	Correction of Erasures	**389**
5.3	Burst Errors and Interleaving of Codes	**401**
5.4	More Details on Compact Discs	**423**
5.5	More Details on CD-ROM	**435**
6	**Enumeration of Isometry Classes**	
6.1	Enumeration of Linear Isometry Classes	**444**
6.2	Indecomposable Linear Codes	**463**
6.3	Cycle Indices of Projective Linear Groups	**476**
6.4	Numerical Data for Linear Isometry Classes	**499**
6.5	Critical Codes	**511**
6.6	Random Generation of Linear Codes	**527**
6.7	Enumeration of Semilinear Isometry Classes	**532**
6.8	Local Isometries	**549**
6.9	Existence and Construction of Normal Bases	**553**
7	**Solving Systems of Diophantine Linear Equations**	
7.1	Lattices	**565**
7.2	Diophantine Equations and Lattices	**568**
7.3	Basic Theory of Lattices	**574**
7.4	Gram–Schmidt Orthogonalization	**577**
7.5	Bounds on Lattice Vectors	**579**
7.6	Lattice Basis Reduction	**586**
7.7	Lattice Point Enumeration	**598**
7.8	Computing the Minimum Distance of Linear Codes	**605**
8	**Linear Codes with a Prescribed Minimum Distance**	
8.1	Minihypers	**616**
8.2	Group Actions on Lattices	**625**

8.3	Prescribing a Group of Automorphisms	**637**
8.4	Linear Codes of Prescribed Type	**640**
8.5	Numerical Results	**644**
9	**The General Case**	
9.1	The Problem	**664**
9.2	Computing with Permutation Groups	**669**
9.3	A Permutation Representation	**676**
9.4	The Lexicographical Order	**682**
9.5	Orderly Generation of Codes	**688**
9.6	The Algorithm Snakes and Ladders	**700**
9.7	Base and Strong Generating Sets	**717**
9.8	The Projective Linear Group	**727**
9.9	The Projective Semilinear Group	**738**
9.10	Numerical Data	**741**
A	**Appendix: The Attached Compact Disc**	
A.1	System Requirements	**755**
A.2	The Installation	**755**
A.3	The Programs	**756**
A.4	The Dynamic Tables	**757**
A.5	The Precomputed Tables: Enumerative Results	**758**
A.6	The Precomputed Tables: Optimal Linear Codes	**759**
A.7	The Programs for Chapter 9	**763**
	References	**771**
	Index	**785**