

Preface	xi
1 Introductory Concepts	1
1.1 Introduction	1
1.2 Basic Definitions	6
1.3 Weight, Minimum Weight, and Maximum-Likelihood Decoding	9
Problems	14
2 Useful Background	17
2.1 Syndrome Decoding	17
2.2 Perfect Codes, Hamming Codes, Sphere-Packing Bound	21
2.3 Packing Radius, Covering Radius, MDS Codes, and Some Bounds	24
2.4 Self-Dual Codes, Golay Codes	29
2.5 Reed-Muller Codes	32
2.6 Puncturing, Extending, and Shortening	35
Problems	36
3 A Double-Error-Correcting BCH Code and a Finite Field of 16 Elements	39
3.1 The Problem	39
3.2 Polynomials	41
3.3 A Finite Field of 16 Elements	44
3.4 Double-Error-Correcting Bose-Chaudhuri-Hocquenghem (BCH) Code	46
Problems	48
4 Finite Fields	51
4.1 Groups	51
4.2 Structure of a Finite Field	54

4.3	Minimal Polynomials	57
4.4	Factoring $x^n - 1$	63
	Problems	64
5	Cyclic Codes	67
5.1	Origin and Definition of Cyclic Codes	67
5.2	How to Find Cyclic Codes: The Generator Polynomial	70
5.3	Generator Polynomial of the Dual Code	73
5.4	Idempotents and Minimal Ideals for Binary Cyclic Codes	76
	Problems	81
6	Group of a Code and Quadratic Residue (QR) Codes	85
6.1	Some Cyclic Codes We Know	85
6.2	Permutation Groups	86
6.3	Group of a Code	87
6.4	Definition of Quadratic Residue (QR) Codes	91
6.5	Extended QR Codes, Square Root Bound, and Groups of QR Codes	96
6.6	Permutation Decoding	100
6.7	Decoding the Golay Code	101
	Problems	105
7	Bose-Chaudhuri-Hocquenghem (BCH) Codes	109
7.1	Cyclic Codes Given in Terms of Roots	109
7.2	Vandermonde Determinants	110
7.3	Definition and Properties of BCH Codes	111
7.4	Reed-Solomon Codes	114
7.5	More on the Minimum Distance	115
7.6	Decoding BCH Codes	116
	Problems	121
8	Weight Distributions	123
8.1	Preliminary Concepts and a Theorem on Weights in Homogeneous Codes	123
8.2	MacWilliams Equations	126
8.3	Pless Power Moments	130
8.4	Gleason Polynomials	134
	Problems	139
9	Designs and Games	143
9.1	Designs	143
9.2	Designs and Codes	147

9.3	Assmus-Mattson Theorem and a Design-Decoding Scheme	149
9.4	Symmetry Codes	153
9.5	Games	156
9.6	Games and Codes	159
9.7	Greedy Codes	160
	Problems	165
10	Some Codes Are Unique	169
10.1	The Hamming Code and the Ternary Golay Code Are Unique	169
10.2	The Steiner System $S(5, 8, 24)$ Is Unique and So Is a Binary $[24, 12, 8]$ Code	173
10.3	"Glue"	176
10.4	Residual Codes and the Griesmer Bound	180
10.5	Some Nonlinear Codes	182
10.6	Z_4 Codes and Their Gray Images	183
	Problems	187
	Appendix	189
	References	199
	Index	203