

ERROR-CORRECTING CODES

SECOND EDITION

W. WESLEY PETERSON

E. J. WELDON, JR.

Technische Hochschule Darmstadt
FACHBEREICH INFORMATIK

B I B L I O T H E K

Inventar-Nr.: 3234

Sachgebiete: _____

Standort: _____

Contents

1 The Coding Problem	1
1.1 The Communication Channel	2
1.2 Some General Remarks on Error-Detecting Error-Correcting Codes	3
1.3 Types of Codes	5
1.4 Block Codes	6
1.5 Tree Codes	10
1.6 The Coding Problem	15
Notes	16
Problems	17
 2 Introduction to Algebra	 19
2.1 Groups	19
2.2 Rings	22
2.3 Fields	23
2.4 Subgroups and Factor Groups	25
2.5 Vector Spaces and Linear Algebras	28
2.6 Matrices	32
Notes	38
Problems	38
 3 Linear Codes	 40
3.1 The Hamming and Lee Metrics	40
3.2 Description of Linear Block Codes by Matrices	42
3.3 Description of Linear Tree Codes by Matrices	47

3.4	The Standard Array	52
3.5	Step-by-Step Decoding of Block Codes	56
3.6	Modular Representation of Linear Block Codes	59
3.7	Linear Block Code Equivalence	62
3.8	Weight Distributions and the MacWilliams Identities	64
3.9	Maximum-Distance-Separable Codes	70
	Notes	72
	Problems	73
4	Error-Correction Capabilities of Linear Codes	76
4.1	Bounds on Minimum Distance for Block Codes	76
4.2	Bounds on the Probability of Error for Block Codes Used on the Binary Symmetric Channel	88
4.3	Discussion of Bounds for Block Codes	99
4.4	Bounds on Minimum Distance for Convolutional Codes	100
4.5	Bounds on the Probability of Error for Convolutional Codes Used on the Binary Symmetric Channel	104
4.6	Bounds for Burst-Error Correcting and Detecting Codes	109
	Notes	115
	Problems	115
5	Important Linear Block Codes	117
5.1	The Hamming Codes	117
5.2	The Golay (23, 12) Code	120
5.3	Optimum Codes for the Binary Symmetric Channel	121
5.4	Binary Codes with Large Minimum Distance	123
5.5	Reed-Muller Codes	125
5.6	Codes Derived from Hadamard Matrices	129
5.7	Product Codes	131
5.8	Graph-Theoretic Codes	136
5.9	Low-Density Codes	138
5.10	Concatenated Codes	139
	Notes	141
	Problems	141
6	Polynomial Rings and Galois Fields	144
6.1	Ideals, Residue Classes, and the Residue Class Ring	144
6.2	Ideals and Residue Classes of Integers	146
6.3	Polynomial Ideals and Residue Classes	148
6.4	The Algebra of Polynomial Residue Classes	150
6.5	Galois Fields	155

6.6	The Multiplicative Group of a Galois Field	157
6.7	Structure of Finite Fields—Summary	161
6.8	Vector Subspaces and Linear Transformations of Finite Fields	164
	Notes	168
	Problems	168
7	Linear Switching Circuits	170
7.1	Definitions	170
7.2	Multiplication and Division of Polynomials	171
7.3	Computations in Polynomial Algebras and Galois Fields	178
7.4	Linear Recurrence Relations and Shift-Register Generators	182
7.5	Z-Transforms, Transfer Functions, and Synthesis	188
7.6	Analysis of a General Linear Finite-State Switching Circuit	195
	Notes	204
	Problems	204
8	Cyclic Codes	206
8.1	Cyclic Codes and Ideals	206
8.2	Matrix Description of Cyclic Codes	212
8.3	Associated-Polynomial Characterization of Cyclic Codes	216
8.4	Hamming Codes	220
8.5	Maximum-Length-Sequence Codes	222
8.6	Some Binary Cyclic Codes	224
8.7	Encoding Procedures	224
8.8	Error Detection with Cyclic Codes	228
8.9	Some Simple Error-Correction Procedures for Short Cyclic Codes	230
8.10	Shortened Cyclic Codes	240
8.11	Code Symmetry	243
8.12	Cyclic Product Codes	250
8.13	Quadratic Residue Codes	254
8.14	Quasi-Cyclic Codes	256
8.15	Codes Based on the Chinese Remainder Theorem	261
	Notes	264
	Problems	265
9	Bose-Chaudhuri-Hocquenghem Codes	269
9.1	The BCH Bound	269
9.2	Definition of the Codes	271
9.3	The True Minimum Weight for BCH Codes	278

9.4	An Error-Correction Procedure	283
9.5	Refinements of the Error-Correction Procedure	288
9.6	Simplifications in the Binary Case	299
9.7	Correction of Erasures and Errors	305
9.8	Negacyclic Codes	307
	Notes	308
	Problems	308
10	Majority-Logic-Decodable Codes	310
10.1	Majority-Logic Decoding	310
10.2	Euclidean Geometry Codes	317
10.3	Projective Geometry Codes	328
10.4	Modifications of the Basic Majority-Logic Decoding Algorithm	333
10.5	Generalized Reed-Muller Codes	340
10.6	Polynomial Codes	350
	Notes	355
	Problems	356
11	Burst-Error-Correcting Cyclic Codes	357
11.1	Analytic Methods of Code Construction	357
11.2	Some Good, Computer-Generated, Burst-Correcting Codes	363
11.3	Decoding	364
11.4	Multiple-Burst Correction	370
11.5	Burst-Error and Random-Error Correction	371
	Notes	372
	Problems	372
12	Synchronization of Block Codes	374
12.1	Codes That Recover Synchronization Only	376
12.2	Codes That Recover Synchronization or Correct Additive Errors	382
12.3	Codes That Recover Synchronization and Correct Additive Errors	386
	Notes	390
	Problems	390
13	Random-Error-Correcting Convolutional Codes	392
13.1	Encoding and Syndrome Calculation	392
13.2	Error Correction and Error Propagation	399

13.3	Single- and Double-Error-Correcting Codes	402
13.4	Self-Orthogonal Codes	404
13.5	Orthogonalizable Codes	409
13.6	Computer-Generated Codes	411
13.7	The Viterbi Decoding Algorithm	412
13.8	Sequential Decoding	421
	Notes	424
	Problems	425
14	Burst-Correcting Convolutional Codes	427
14.1	Some Definitions	427
14.2	Berlekamp-Preparata-Massey Codes	430
14.3	Iwadare Codes	434
14.4	Low-Rate Codes	440
14.5	Codes for Correcting Bursts and Random Errors	442
	Notes	446
	Problems	447
15	Arithmetic Codes	449
15.1	Definition of Arithmetic Error and Distance	449
15.2	Properties of Arithmetic Weight for the Binary Case	451
15.3	The Arithmetic Codes	453
15.4	Perfect, Arithmetic, Single-Error Correcting Codes	456
15.5	Arithmetic Codes with Large Minimum Distance	457
15.6	Self-Complementing $AN + B$ Codes	460
15.7	Implementing AN and $AN + B$ Codes	461
15.8	Separate Adder and Checker	463
	Notes	465
	Problems	465
Appendix A	Inequalities Involving Binomial Coefficients	466
Appendix B	A Short Table of the Entropy Function (Base 10) and Its First Derivative	470
Appendix C	Tables of Irreducible Polynomials over $GF(2)$	472
Appendix D	A List of Binary Cyclic Codes of Odd Length	493
	Selected Bibliography	535
	Index	549