Signal Design for Good Correlation

For Wireless Communication, Cryptography, and Radar

SOLOMON W. GOLOMB
University of Southern California

GUANG GONG
University of Waterloo, Ontario

CAMBRIDGE
UNIVERSITY PRESS

Contents

Preface page xi

Acknowledgments xiii

Historical Introduction xv

1 General Properties of Correlation 1

1.1 What is correlation? 1

1.2 Continuous correlation 2

1.3 Binary correlation 2

1.4 Complex correlation 3

1.5 Mutual orthogonality 3

1.6 The simplex bound on mutual negative correlation 4

1.7 Autocorrelation 6

1.8 Crosscorrelation 7

2 Applications of Correlation to the Communication of Information 10

2.1 The maximum likelihood detector 10

2.2 Coherent versus incoherent detection 12

2.3 Orthogonal, biorthogonal, and simplex codes 14

2.4 Hadamard matrices and code construction 15

2.5 Cyclic Hadamard matrices 18

3 Finite Fields 22

3.1 Algebraic structures 22

3.2 Construction of $GF(p^n)$ 31

3.3 The basic theory of finite fields 34

3.4 Minimal polynomials 41

3.5 Trace functions 52

3.6 Powers of trace functions 58

3.7 The numbers of irreducible polynomials and coset leaders 69

Appendix A: A Maple program for step 3 in Algorithm 3.1 72
Appendix B: Primitive polynomials 72
Appendix C: Minimal polynomials 77
Exercises for Chapter 3 79
4 Feedback Shift Register Sequences 81
4.1 Feedback shift registers 82
4.2 Definition of LFSR sequences in terms of polynomial rings 90
4.3 Minimal polynomials and periods 94
4.4 Decomposition of LFSR sequences 103
4.5 The matrix representation 106
4.6 Trace representation of LFSRs 108
4.7 Generating functions of LFSRs 112
Exercises for Chapter 4 114
5 Randomness Measurements and m-Sequences 117
5.1 Golomb's randomness postulates and randomness criteria 117
5.2 Randomness properties of m-sequences 127
5.3 Interleaved structure of m-sequences 135
5.4 Trinomial property 145
5.5 Constant-on-cosets property 148
5.6 Two-tuple balance property 152
5.7 Classification of binary sequences of period $2^n - 1$ 155
Exercises for Chapter 5 159
6 Transforms of Sequences and Functions 162
6.1 The (discrete) Fourier transform 162
6.2 Trace representation 166
6.3 Linear spans and spectral sequences 174
6.4 One-to-one correspondence between sequences and functions 177
6.5 Hadamard transform and convolution transform 185
6.6 Correlation of functions 190
6.7 Laws of the Hadamard transform and convolution transform 193
6.8 The matrix representation of the DFT and the Hadamard transform 197
Exercises for Chapter 6 199
7 Cyclic Difference Sets and Binary Sequences with Two-Level Autocorrelation 202
7.1 Cyclic difference sets and their relationship to binary sequences with two-level autocorrelation 202
7.2 More results about C 207
7.3 Fourier spectral constraints 211
Exercises for Chapter 7 218

8 Cyclic Hadamard Sequences, Part 1 219
8.1 Constructions with subfield decomposition 220
8.2 GMW constructions 234
8.3 Statistical properties of GMW sequences of all types 248
8.4 Linear spans of GMW sequences of all types 250
8.5 Shift-distinct sequences from GMW constructions 255
8.6 Implementation aspects of GMW constructions 257
Exercises for Chapter 8 264
9 Cyclic Hadamard Sequences, Part 2 267
9.1 Multiple trace term sequences 267
9.2 Hyperoval constructions 282
9.3 Kasami power function construction 294
9.4 The iterative decimation Hadamard transform 303
Appendix: Known 2-level autocorrelation sequences of periods 1023, 2047, and 4095 and their trace representations 318
Exercises for Chapter 9 321
10 Signal Sets with Low Crosscorrelation 323
10.1 Crosscorrelation, signal sets, and boolean functions 323
10.2 Odd case: Gold-pair signal sets and their generalization 336
10.3 Even case: Kasami (small) signal sets and their generalization 344
10.4 Even case: Bent function signal sets 353
10.5 Interleaved construction of signal sets 363
10.6 $\mathbb{Z}_4$ signal sets 371
Exercises for Chapter 10 380
11 Correlation of Boolean Functions 382
11.1 Invariants, resiliency, and nonlinearity 383
11.2 Dual functions and resiliency 392
11.3 Dual functions, additive autocorrelation, and the propagation property 395
Exercises for Chapter 11 401
12 Applications to Radar, Sonar, Synchronization, and CDMA 402
12.1 Overview 402
12.2 Types of signals and correlations 403
12.3 Barker sequences 404
12.4 Generalized Barker sequences 405
12.5 Huffman's impulse-equivalent pulse trains 406
12.6 Pulse patterns and optimal rulers 408
12.7 Perfect circular rulers from cyclic projective planes 412
12.8 Two-dimensional pulse patterns 415
12.9 Periodic modulation 417

12.10 The application to CDMA wireless technology 419
Exercises for Chapter 12 421

Bibliography 423
Index 433