

DIGITAL COMMUNICATIONS

DIGITAL COMMUNICATIONS

Fundamentals and Applications

BERNARD SKLAR

*The Aerospace Corporation, El Segundo, California
and
University of California, Los Angeles*

FENWICK LIBRARY
GEORGE MASON UNIVERSITY
FAIRFAX, VA.



PRENTICE HALL

Englewood Cliffs, New Jersey 07632

Library of Congress Cataloging-in-Publication Data

SKLAR, BERNARD (date)

Digital communications.

Bibliography: p.

Includes index.

1. Digital communications. I. Title.

TK5103.7.S55 1988 621.38'0413 87-1316

ISBN 0-13-211939-0

Editorial/production supervision and
interior design: Reynold Rieger
Cover design: Wanda Lubelska Design
Manufacturing buyers: Gordon Osbourne and Paula Benevento



© 1988 by Prentice Hall
A Division of Simon & Schuster
Englewood Cliffs, New Jersey 07632

All rights reserved. No part of this book may be
reproduced, in any form or by any means,
without permission in writing from the publisher.

Printed in the United States of America

10 9 8 7 6 5 4 3 2

ISBN 0-13-211939-0 025

Prentice-Hall International (UK) Limited, *London*
Prentice-Hall of Australia Pty. Limited, *Sydney*
Prentice-Hall Canada Inc., *Toronto*
Prentice-Hall Hispanoamericana, S.A., *Mexico*
Prentice-Hall of India Private Limited, *New Delhi*
Prentice-Hall of Japan, Inc., *Tokyo*
Simon & Schuster Asia Pte. Ltd., *Singapore*
Editora Prentice-Hall do Brasil, Ltda., *Rio de Janeiro*

TK

5109.7

, 555

1988

1
0
7

*To my mother, Ruth Sklar,
the memory of my father, Julius Sklar,
my wife, Gwen, and our children,
Debra, Sharon, and Dean*

Contents

PREFACE

xxi

1 SIGNALS AND SPECTRA

1

- 1.1 Digital Communication Signal Processing, 3
 - 1.1.1 *Why Digital?*, 3
 - 1.1.2 *Typical Block Diagram and Transformations*, 4
 - 1.1.3 *Basic Digital Communication Nomenclature*, 9
 - 1.1.4 *Digital versus Analog Performance Criteria*, 11
- 1.2 Classification of Signals, 11
 - 1.2.1 *Deterministic and Random Signals*, 11
 - 1.2.2 *Periodic and Nonperiodic Signals*, 12
 - 1.2.3 *Analog and Discrete Signals*, 12
 - 1.2.4 *Energy and Power Signals*, 12
 - 1.2.5 *The Unit Impulse Function*, 13
- 1.3 Spectral Density, 14
 - 1.3.1 *Energy Spectral Density*, 14
 - 1.3.2 *Power Spectral Density*, 15
- 1.4 Autocorrelation, 17
 - 1.4.1 *Autocorrelation of an Energy Signal*, 17
 - 1.4.2 *Autocorrelation of a Periodic (Power) Signal*, 17
- 1.5 Random Signals, 18
 - 1.5.1 *Random Variables*, 18
 - 1.5.2 *Random Processes*, 20

vii

1.5.3	Time Averaging and Ergodicity,	22
1.5.4	Power Spectral Density of a Random Process,	23
1.5.5	Noise in Communication Systems,	27
1.6	Signal Transmission through Linear Systems,	30
1.6.1	Impulse Response,	31
1.6.2	Frequency Transfer Function,	31
1.6.3	Distortionless Transmission,	32
1.6.4	Signals, Circuits, and Spectra,	38
1.7	Bandwidth of Digital Data,	41
1.7.1	Baseband versus Bandpass,	41
1.7.2	The Bandwidth Dilemma,	43
1.8	Conclusion,	46
	References,	46
	Problems,	47

2 FORMATTING AND BASEBAND TRANSMISSION

51

2.1	Baseband Systems,	54
2.2	Formatting Textual Data (Character Coding),	55
2.3	Messages, Characters, and Symbols,	55
2.3.1	Example of Messages, Characters, and Symbols,	55
2.4	Formatting Analog Information,	59
2.4.1	The Sampling Theorem,	59
2.4.2	Aliasing,	66
2.4.3	Signal Interface for a Digital System,	69
2.5	Sources of Corruption,	70
2.5.1	Sampling and Quantizing Effects,	70
2.5.2	Channel Effects,	71
2.5.3	Signal-to-Noise Ratio for Quantized Pulses,	72
2.6	Pulse Code Modulation,	73
2.7	Uniform and Nonuniform Quantization,	74
2.7.1	Statistics of Speech Amplitudes,	74
2.7.2	Nonuniform Quantization,	76
2.7.3	Companding Characteristics,	77
2.8	Baseband Transmission,	78
2.8.1	Waveform Representation of Binary Digits,	78
2.8.2	PCM Waveform Types,	78
2.8.3	Spectral Attributes of PCM Waveforms,	82
2.9	Detection of Binary Signals in Gaussian Noise,	83
2.9.1	Maximum Likelihood Receiver Structure,	85
2.9.2	The Matched Filter,	88
2.9.3	Correlation Realization of the Matched Filter,	90
2.9.4	Application of the Matched Filter,	91
2.9.5	Error Probability Performance of Binary Signaling,	92

viii

Contents

2.10	Multilevel Baseband Transr	
2.10.1	PCM Word Size,	97
2.11	Intersymbol Interference,	
2.11.1	Pulse Shaping to Rec	
2.11.2	Equalization,	104
2.12	Partial Response Signaling,	
2.12.1	Duobinary Signaling,	
2.12.2	Duobinary Decoding	
2.12.3	Precoding,	108
2.12.4	Duobinary Equivaler	
2.12.5	Comparison of Bina	
	Signaling,	111
2.12.6	Polybinary Signaling	
2.13	Conclusion,	112
	References,	113
	Problems,	113

3 BANDPASS MODULATION

3.1	Why Modulate?,	118
3.2	Signals and Noise,	119
3.2.1	Noise in Radio Co	
3.2.2	A Geometric View	
3.3	Digital Bandpass Modula	
3.3.1	Phase Shift Keyin,	
3.3.2	Frequency Shift K	
3.3.3	Amplitude Shift K	
3.3.4	Amplitude Phase	
3.3.5	Waveform Ampliti	
3.4	Detection of Signals in C	
3.4.1	Decision Regions	
3.4.2	Correlation Recei	
3.5	Coherent Detection,	121
3.5.1	Coherent Detecti	
3.5.2	Sampled Matche	
3.5.3	Coherent Detecti	
	Keying,	142
3.5.4	Coherent Detecti	
3.6	Noncoherent Detection	
3.6.1	Detection of Diff	
3.6.2	Binary Different	
3.6.3	Noncoherent De	
3.6.4	Minimum Requi	
	Orthogonal FSK	

Contents

2.10	Multilevel Baseband Transmission,	95
2.10.1	PCM Word Size,	97
2.11	Intersymbol Interference,	98
2.11.1	Pulse Shaping to Reduce ISI,	100
2.11.2	Equalization,	104
2.12	Partial Response Signaling,	106
2.12.1	Duobinary Signaling,	106
2.12.2	Duobinary Decoding,	107
2.12.3	Precoding,	108
2.12.4	Duobinary Equivalent Transfer Function,	109
2.12.5	Comparison of Binary with Duobinary Signaling,	111
2.12.6	Polybinary Signaling,	112
2.13	Conclusion,	112
	References,	113
	Problems,	113

3 BANDPASS MODULATION AND DEMODULATION

117

3.1	Why Modulate?,	118
3.2	Signals and Noise,	119
3.2.1	Noise in Radio Communication Systems,	119
3.2.2	A Geometric View of Signals and Noise,	120
3.3	Digital Bandpass Modulation Techniques,	127
3.3.1	Phase Shift Keying,	130
3.3.2	Frequency Shift Keying,	130
3.3.3	Amplitude Shift Keying,	131
3.3.4	Amplitude Phase Keying,	131
3.3.5	Waveform Amplitude Coefficient,	132
3.4	Detection of Signals in Gaussian Noise,	132
3.4.1	Decision Regions,	132
3.4.2	Correlation Receiver,	133
3.5	Coherent Detection,	138
3.5.1	Coherent Detection of PSK,	138
3.5.2	Sampled Matched Filter,	139
3.5.3	Coherent Detection of Multiple Phase Shift Keying,	142
3.5.4	Coherent Detection of FSK,	145
3.6	Noncoherent Detection,	146
3.6.1	Detection of Differential PSK,	146
3.6.2	Binary Differential PSK Example,	148
3.6.3	Noncoherent Detection of FSK,	150
3.6.4	Minimum Required Tone Spacing for Noncoherent Orthogonal FSK Signaling,	152

3.7	Error Performance for Binary Systems,	155
3.7.1	<i>Probability of Bit Error for Coherently Detected BPSK,</i>	155
3.7.2	<i>Probability of Bit Error for Coherently Detected Differentially Encoded PSK,</i>	160
3.7.3	<i>Probability of Bit Error for Coherently Detected FSK,</i>	161
3.7.4	<i>Probability of Bit Error for Noncoherently Detected FSK,</i>	162
3.7.5	<i>Probability of Bit Error for DPSK,</i>	164
3.7.6	<i>Comparison of Bit Error Performance for Various Modulation Types,</i>	166
3.8	M-ary Signaling and Performance,	167
3.8.1	<i>Ideal Probability of Bit Error Performance,</i>	167
3.8.2	<i>M-ary Signaling,</i>	167
3.8.3	<i>Vectorial View of MPSK Signaling,</i>	170
3.8.4	<i>BPSK and QPSK Have the Same Bit Error Probability,</i>	171
3.8.5	<i>Vectorial View of MFSK Signaling,</i>	172
3.9	Symbol Error Performance for M-ary Systems ($M > 2$),	176
3.9.1	<i>Probability of Symbol Error for MPSK,</i>	176
3.9.2	<i>Probability of Symbol Error for MFSK,</i>	177
3.9.3	<i>Bit Error Probability versus Symbol Error Probability for Orthogonal Signals,</i>	180
3.9.4	<i>Bit Error Probability versus Symbol Error Probability for Multiple Phase Signaling,</i>	181
3.9.5	<i>Effects of Intersymbol Interference,</i>	182
3.10	Conclusion,	182
	References,	182
	Problems,	183

4 COMMUNICATIONS LINK ANALYSIS

187

4.1	What the System Link Budget Tells the System Engineer,	188
4.2	The Channel,	189
4.2.1	<i>The Concept of Free Space,</i>	189
4.2.2	<i>Signal-to-Noise Ratio Degradation,</i>	190
4.2.3	<i>Sources of Signal Loss and Noise,</i>	190
4.3	Received Signal Power and Noise Power,	195
4.3.1	<i>The Range Equation,</i>	195
4.3.2	<i>Received Signal Power as a Function of Frequency,</i>	199
4.3.3	<i>Path Loss Is Frequency Dependent,</i>	200
4.3.4	<i>Thermal Noise Power,</i>	202

x

Contents

- 4.4 Link Budget Analysis, 204
 - 4.4.1 *Two E_b/N_0 Values of Interest*, 205
 - 4.4.2 *Link Budgets Are Typically Calculated in Decibels*, 206
 - 4.4.3 *How Much Link Margin Is Enough?*, 207
 - 4.4.4 *Link Availability*, 209
- 4.5 Noise Figure, Noise Temperature, and System Temperature, 213
 - 4.5.1 *Noise Figure*, 213
 - 4.5.2 *Noise Temperature*, 215
 - 4.5.3 *Line Loss*, 216
 - 4.5.4 *Composite Noise Figure and Composite Noise Temperature*, 218
 - 4.5.5 *System Effective Temperature*, 220
 - 4.5.6 *Sky Noise Temperature*, 224
- 4.6 Sample Link Analysis, 228
 - 4.6.1 *Link Budget Details*, 228
 - 4.6.2 *Receiver Figure-of-Merit*, 230
 - 4.6.3 *Received Isotropic Power*, 231
- 4.7 Satellite Repeaters, 232
 - 4.7.1 *Nonregenerative Repeaters*, 232
 - 4.7.2 *Nonlinear Repeater Amplifiers*, 236
- 4.8 System Trade-Offs, 238
- 4.9 Conclusion, 239
 - References, 239
 - Problems, 240

5 CHANNEL CODING: PART 1

245

- 5.1 Waveform Coding, 246
 - 5.1.1 *Antipodal and Orthogonal Signals*, 247
 - 5.1.2 *M-ary Signaling*, 249
 - 5.1.3 *Waveform Coding with Correlation Detection*, 249
 - 5.1.4 *Orthogonal Codes*, 251
 - 5.1.5 *Biorthogonal Codes*, 255
 - 5.1.6 *Transorthogonal (Simplex) Codes*, 257
- 5.2 Types of Error Control, 258
 - 5.2.1 *Terminal Connectivity*, 258
 - 5.2.2 *Automatic Repeat Request*, 259
- 5.3 Structured Sequences, 260
 - 5.3.1 *Channel Models*, 261
 - 5.3.2 *Code Rate and Redundancy*, 263
 - 5.3.3 *Parity-Check Codes*, 263
 - 5.3.4 *Coding Gain*, 266

5.4	Linear Block Codes, 269
5.4.1	Vector Spaces, 269
5.4.2	Vector Subspaces, 270
5.4.3	A (6, 3) Linear Block Code Example, 271
5.4.4	Generator Matrix, 272
5.4.5	Systematic Linear Block Codes, 273
5.4.6	Parity-Check Matrix, 275
5.4.7	Syndrome Testing, 276
5.4.8	Error Correction, 277
5.5	Coding Strength, 280
5.5.1	Weight and Distance of Binary Vectors, 280
5.5.2	Minimum Distance of a Linear Code, 281
5.5.3	Error Detection and Correction, 281
5.5.4	Visualization of a 6-Tuple Space, 285
5.5.5	Erasure Correction, 287
5.6	Cyclic Codes, 288
5.6.1	Algebraic Structure of Cyclic Codes, 288
5.6.2	Binary Cyclic Code Properties, 290
5.6.3	Encoding in Systematic Form, 290
5.6.4	Circuit for Dividing Polynomials, 292
5.6.5	Systematic Encoding with an $(n - k)$ -Stage Shift Register, 294
5.6.6	Error Detection with an $(n - k)$ -Stage Shift Register, 296
5.7	Well-Known Block Codes, 298
5.7.1	Hamming Codes, 298
5.7.2	Extended Golay Code, 301
5.7.3	BCH Codes, 301
5.7.4	Reed-Solomon Codes, 304
5.8	Conclusion, 308
	References, 308
	Problems, 309

6 CHANNEL CODING: PART 2

314

6.1	Convolutional Encoding, 315
6.2	Convolutional Encoder Representation, 317
6.2.1	Connection Representation, 318
6.2.2	State Representation and the State Diagram, 322
6.2.3	The Tree Diagram, 324
6.2.4	The Trellis Diagram, 326
6.3	Formulation of the Convolutional Decoding Problem, 327
6.3.1	Maximum Likelihood Decoding, 327
6.3.2	Channel Models: Hard versus Soft Decisions, 329
6.3.3	The Viterbi Convolutional Decoding Algorithm, 333

xii

Contents

6.3.4	An Example of Convolutional Coding, 335
6.3.5	Path Metric, 336
6.4	Properties of Convolutional Codes, 337
6.4.1	Distance Properties, 337
6.4.2	Systematic Convolutional Codes, 338
6.4.3	Catastrophic Convolutional Codes, 339
6.4.4	Performance of Convolutional Codes, 340
6.4.5	Coding Rate, 340
6.4.6	Best Known Convolutional Codes, 341
6.4.7	Convolutional Codes and the Viterbi Algorithm, 342
6.5	Other Convolutional Codes, 343
6.5.1	Sequences, 343
6.5.2	Comparison of Convolutional Codes, 344
6.5.3	Feedback Convolutional Codes, 345
6.6	Interleaving and Convolutional Codes, 346
6.6.1	Block Interleaving, 346
6.6.2	Convolutional Interleaving, 347
6.6.3	Concatenated Codes, 348
6.7	Coding and Interleaving in an Audio System, 349
6.7.1	CIRC Encoder, 349
6.7.2	CIRC Decoder, 350
6.7.3	Interpolation, 351
6.8	Conclusion, 352
	References, 352
	Problems, 376

7 MODULATION AND TRANSMISSION

7.1	Goals of the Chapter, 353
7.2	Error Probability, 353
7.3	Nyquist Minimum Bandwidth, 354
7.4	Shannon-Hartley Theorem, 355
7.4.1	Shannon's Theorem, 355
7.4.2	Entropy, 356
7.4.3	Equivalences, 357
7.5	Bandwidth-Efficient Modulation, 358
7.5.1	Bandwidth-Efficient Modulation, 358
7.5.2	Analog Modulation, 359
7.6	Power-Limited Channels, 360

Contents

6.3.4	<i>An Example of Viterbi Convolutional Decoding,</i>	333
6.3.5	<i>Path Memory and Synchronization,</i>	337
6.4	Properties of Convolutional Codes,	338
6.4.1	<i>Distance Properties of Convolutional Codes,</i>	338
6.4.2	<i>Systematic and Nonsystematic Convolutional Codes,</i>	342
6.4.3	<i>Catastrophic Error Propagation in Convolutional Codes,</i>	342
6.4.4	<i>Performance Bounds for Convolutional Codes,</i>	344
6.4.5	<i>Coding Gain,</i>	345
6.4.6	<i>Best Known Convolutional Codes,</i>	347
6.4.7	<i>Convolutional Code Rate Trade-Off,</i>	348
6.5	Other Convolutional Decoding Algorithms,	350
6.5.1	<i>Sequential Decoding,</i>	350
6.5.2	<i>Comparisons and Limitations of Viterbi and Sequential Decoding,</i>	354
6.5.3	<i>Feedback Decoding,</i>	355
6.6	Interleaving and Concatenated Codes,	357
6.6.1	<i>Block Interleaving,</i>	360
6.6.2	<i>Convolutional Interleaving,</i>	362
6.6.3	<i>Concatenated Codes,</i>	365
6.7	Coding and Interleaving Applied to the Compact Disc Digital Audio System,	366
6.7.1	<i>CIRC Encoding,</i>	367
6.7.2	<i>CIRC Decoding,</i>	369
6.7.3	<i>Interpolation and Muting,</i>	371
6.8	Conclusion,	374
	References,	374
	Problems,	376

7 MODULATION AND CODING TRADE-OFFS

381

7.1	Goals of the Communications System Designer,	382
7.2	Error Probability Plane,	383
7.3	Nyquist Minimum Bandwidth,	385
7.4	Shannon-Hartley Capacity Theorem,	385
7.4.1	<i>Shannon Limit,</i>	387
7.4.2	<i>Entropy,</i>	389
7.4.3	<i>Equivocation and Effective Transmission Rate,</i>	391
7.5	Bandwidth-Efficiency Plane,	393
7.5.1	<i>Bandwidth Efficiency of MPSK and MFSK Modulation,</i>	395
7.5.2	<i>Analogies between Bandwidth-Efficiency and Error Probability Planes,</i>	396
7.6	Power-Limited Systems,	396

Contents

xiii

- 7.7 Bandwidth-Limited Systems, 397
- 7.8 Modulation and Coding Trade-Offs, 397
- 7.9 Bandwidth-Efficient Modulations, 399
 - 7.9.1 QPSK and Offset QPSK Signaling, 399
 - 7.9.2 Minimum Shift Keying, 403
 - 7.9.3 Quadrature Amplitude Modulation, 407
- 7.10 Modulation and Coding for Bandlimited Channels, 410
 - 7.10.1 Commercial Telephone Modems, 411
 - 7.10.2 Signal Constellation Boundaries, 412
 - 7.10.3 Higher-Dimensional Signal Constellations, 412
 - 7.10.4 Higher-Density Lattice Structures, 415
 - 7.10.5 Combined-Gain: N-Sphere Mapping and Dense Lattice, 416
 - 7.10.6 Trellis-Coded Modulation, 417
 - 7.10.7 Trellis-Coding Example, 420
- 7.11 Conclusion, 424
- References, 425
- Problems, 426

8 SYNCHRONIZATION

429

Maurice A. King, Jr.

- 8.1 Synchronization in the Context of Digital Communications, 430
 - 8.1.1 What It Means to Be Synchronized, 430
 - 8.1.2 Costs versus Benefits of Synchronization Levels, 432
- 8.2 Receiver Synchronization, 434
 - 8.2.1 Coherent Systems: Phase-Locked Loops, 434
 - 8.2.2 Symbol Synchronization, 453
 - 8.2.3 Frame Synchronization, 460
- 8.3 Network Synchronization, 464
 - 8.3.1 Open-Loop Transmitter Synchronization, 465
 - 8.3.2 Closed-Loop Transmitter Synchronization, 468
- 8.4 Conclusion, 470
- References, 471
- Problems, 472

9 MULTIPLEXING AND MULTIPLE ACCESS

475

- 9.1 Allocation of the Communications Resource, 476
 - 9.1.1 Frequency-Division Multiplexing/Multiple Access, 478

- 9.1.2 Time-Division M
- 9.1.3 Communications
- 9.1.4 Performance C
- TDMA, 488
- 9.1.5 Code-Division M
- 9.1.6 Space-Division
- Access, 493

9.2 Multiple Access Comm

Architecture, 495

9.2.1 Multiple Acces

9.2.2 Demand-Assig

9.3 Access Algorithms,

9.3.1 ALOHA, 498

9.3.2 Slotted ALOH

9.3.3 Reservation-A

9.3.4 Performance C

and R-ALOHA

9.3.5 Polling Techn

9.4 Multiple Access Tec

INTELSAT, 507

9.4.1 Preassigned

Operation, 507

9.4.2 MCPC Mode

Satellite, 511

9.4.3 SPADE Oper

9.4.4 TDMA in IN

9.4.5 Satellite-Swi

9.5 Multiple Access Tec

9.5.1 Carrier-Sens

9.5.2 Token-Ring

9.5.3 Performance

and Token-R

9.6 Conclusion, 531

References, 532

Problems, 533

10 SPREAD-SPECTRUM

10.1 Spread-Spectrum

10.1.1 The Benefi

Systems,

10.1.2 Model for

Rejection,

10.1.3 A Catalog

10.1.4 Historical

9.1.2	<i>Time-Division Multiplexing/Multiple Access,</i>	484
9.1.3	<i>Communications Resource Channelization,</i>	487
9.1.4	<i>Performance Comparison of FDMA and TDMA,</i>	488
9.1.5	<i>Code-Division Multiple Access,</i>	491
9.1.6	<i>Space-Division and Polarization-Division Multiple Access,</i>	493
9.2	Multiple Access Communications System and Architecture,	495
9.2.1	<i>Multiple Access Information Flow,</i>	496
9.2.2	<i>Demand-Assignment Multiple Access,</i>	497
9.3	Access Algorithms,	498
9.3.1	<i>ALOHA,</i>	498
9.3.2	<i>Slotted ALOHA,</i>	500
9.3.3	<i>Reservation-ALOHA,</i>	502
9.3.4	<i>Performance Comparison of S-ALOHA and R-ALOHA,</i>	503
9.3.5	<i>Polling Techniques,</i>	505
9.4	Multiple Access Techniques Employed with INTELSAT,	507
9.4.1	<i>Preassigned FDM/FM/FDMA or MCPC Operation,</i>	508
9.4.2	<i>MCPC Modes of Accessing an INTELSAT Satellite,</i>	510
9.4.3	<i>SPADE Operation,</i>	511
9.4.4	<i>TDMA in INTELSAT,</i>	516
9.4.5	<i>Satellite-Switched TDMA in INTELSAT,</i>	523
9.5	Multiple Access Techniques for Local Area Networks,	526
9.5.1	<i>Carrier-Sense Multiple Access Networks,</i>	526
9.5.2	<i>Token-Ring Networks,</i>	528
9.5.3	<i>Performance Comparison of CSMA/CD and Token-Ring Networks,</i>	530
9.6	Conclusion,	531
	References,	532
	Problems,	533

10 SPREAD-SPECTRUM TECHNIQUES

536

10.1	Spread-Spectrum Overview,	537
10.1.1	<i>The Beneficial Attributes of Spread-Spectrum Systems,</i>	538
10.1.2	<i>Model for Spread-Spectrum Interference Rejection,</i>	542
10.1.3	<i>A Catalog of Spreading Techniques,</i>	543
10.1.4	<i>Historical Background,</i>	544

10.2	Pseudonoise Sequences, 546
10.2.1	Randomness Properties, 546
10.2.2	Shift Register Sequences, 547
10.2.3	PN Autocorrelation Function, 548
10.3	Direct-Sequence Spread-Spectrum Systems, 549
10.3.1	Example of Direct Sequencing, 550
10.3.2	Processing Gain and Performance, 552
10.4	Frequency Hopping Systems, 555
10.4.1	Frequency Hopping Example, 557
10.4.2	Robustness, 558
10.4.3	Frequency Hopping with Diversity, 559
10.4.4	Fast Hopping versus Slow Hopping, 560
10.4.5	FFH/MFSK Demodulator, 562
10.5	Synchronization, 562
10.5.1	Acquisition, 563
10.5.2	Tracking, 568
10.6	Spread-Spectrum Applications, 571
10.6.1	Code-Division Multiple Access, 571
10.6.2	Multipath Channels, 573
10.6.3	The Jamming Game, 574
10.7	Further Jamming Considerations, 579
10.7.1	Broadband Noise Jamming, 579
10.7.2	Partial-Band Noise Jamming, 581
10.7.3	Multiple-Tone Jamming, 583
10.7.4	Pulse Jamming, 584
10.7.5	Repeat-Back Jamming, 586
10.7.6	BLADES System, 588
10.8	Conclusion, 589
	References, 589
	Problems, 591

11 SOURCE CODING

Fredric J. Harris

11.1	Sources, 596
11.1.1	Discrete Sources, 596
11.1.2	Waveform Sources, 601
11.2	Amplitude Quantizing, 603
11.2.1	Quantizing Noise, 605
11.2.2	Uniform Quantizing, 608
11.2.3	Saturation, 611
11.2.4	Dithering, 614
11.2.5	Nonuniform Quantizing, 617
11.3	Differential Pulse Code Modulation, 627
11.3.1	One-Tap Prediction, 630
11.3.2	N-Tap Prediction, 631

xvi

595

Contents

11.3.3	Delta Modulation, 6
11.3.4	Adaptive Prediction, 6
11.4	Block Coding, 643
11.4.1	Vector Quantizing, 643
11.4.2	Transform Coding, 643
11.4.3	Quantization for Tra, 643
11.4.4	Subband Coding, 643
11.5	Synthesis/Analysis Coding, 650
11.5.1	Vocoders, 650
11.5.2	Linear Predictive Co, 650
11.6	Redundancy-Reducing Co, 650
11.6.1	Properties of Codes, 650
11.6.2	Huffman Code, 650
11.6.3	Run-Length Codes, 650
11.7	Conclusion, 663
	References, 663
	Problems, 664

12 ENCRYPTION AND DEC

12.1	Models, Goals, and Ea, 669
12.1.1	A Model of the, 669
12.1.2	System Goals, 669
12.1.3	Classic Threats, 669
12.1.4	Classic Ciphers, 669
12.2	The Secrecy of a Ciph, 669
12.2.1	Perfect Secrecy, 669
12.2.2	Entropy and Ea, 669
12.2.3	Rate of a Lang, 669
12.2.4	Unicity Distan, 669
12.3	Practical Security, 669
12.3.1	Confusion and, 669
12.3.2	Substitution, 669
12.3.3	Permutation, 669
12.3.4	Product Ciph, 669
12.3.5	The Data Enc, 669
12.4	Stream Encryption, 669
12.4.1	Example of F, 669
12.4.2	Feedback Sh, 669
12.4.3	Vulnerabilit, 669
	Registers, 669
	Synchronou, 669
	Encryption, 669

Contents

	11.3.3	<i>Delta Modulation,</i>	633
	11.3.4	<i>Adaptive Prediction,</i>	639
11.4		Block Coding,	643
	11.4.1	<i>Vector Quantizing,</i>	643
	11.4.2	<i>Transform Coding,</i>	645
	11.4.3	<i>Quantization for Transform Coding,</i>	647
	11.4.4	<i>Subband Coding,</i>	647
11.5		Synthesis/Analysis Coding,	649
	11.5.1	<i>Vocoders,</i>	650
	11.5.2	<i>Linear Predictive Coding,</i>	653
11.6		Redundancy-Reducing Coding,	653
	11.6.1	<i>Properties of Codes,</i>	655
	11.6.2	<i>Huffman Code,</i>	657
	11.6.3	<i>Run-Length Codes,</i>	660
11.7		Conclusion,	663
		References,	663
		Problems,	664

12 ENCRYPTION AND DECRYPTION

668

12.1		Models, Goals, and Early Cipher Systems,	669
	12.1.1	<i>A Model of the Encryption and Decryption Process,</i>	669
	12.1.2	<i>System Goals,</i>	671
	12.1.3	<i>Classic Threats,</i>	671
	12.1.4	<i>Classic Ciphers,</i>	672
12.2		The Secrecy of a Cipher System,	675
	12.2.1	<i>Perfect Secrecy,</i>	675
	12.2.2	<i>Entropy and Equivocation,</i>	678
	12.2.3	<i>Rate of a Language and Redundancy,</i>	680
	12.2.4	<i>Unicity Distance and Ideal Secrecy,</i>	680
12.3		Practical Security,	683
	12.3.1	<i>Confusion and Diffusion,</i>	683
	12.3.2	<i>Substitution,</i>	683
	12.3.3	<i>Permutation,</i>	685
	12.3.4	<i>Product Cipher System,</i>	686
	12.3.5	<i>The Data Encryption Standard,</i>	687
12.4		Stream Encryption,	694
	12.4.1	<i>Example of Key Generation Using a Linear Feedback Shift Register,</i>	694
	12.4.2	<i>Vulnerabilities of Linear Feedback Shift Registers,</i>	695
	12.4.3	<i>Synchronous and Self-Synchronous Stream Encryption Systems,</i>	697

- 12.5 Public Key Cryptosystems, 698
 - 12.5.1 *Signature Authentication Using a Public Key Cryptosystem*, 699
 - 12.5.2 *A Trapdoor One-Way Function*, 700
 - 12.5.3 *The Rivest-Shamir-Adelman Scheme*, 701
 - 12.5.4 *The Knapsack Problem*, 703
 - 12.5.5 *A Public Key Cryptosystem Based on a Trapdoor Knapsack*, 705
- 12.6 Conclusion, 707
- References, 707
- Problems, 708

A A REVIEW OF FOURIER TECHNIQUES

710

- A.1 Signals, Spectra, and Linear Systems, 710
- A.2 Fourier Techniques for Linear System Analysis, 711
 - A.2.1 *Fourier Series Transform*, 713
 - A.2.2 *Spectrum of a Pulse Train*, 716
 - A.2.3 *Fourier Integral Transform*, 719
- A.3 Fourier Transform Properties, 720
 - A.3.1 *Time Shifting Property*, 720
 - A.3.2 *Frequency Shifting Property*, 720
- A.4 Useful Functions, 721
 - A.4.1 *Unit Impulse Function*, 721
 - A.4.2 *Spectrum of a Sinusoid*, 721
- A.5 Convolution, 722
 - A.5.1 *Graphical Illustration of Convolution*, 726
 - A.5.2 *Time Convolution Property*, 726
 - A.5.3 *Frequency Convolution Property*, 726
 - A.5.4 *Convolution of a Function with a Unit Impulse*, 728
 - A.5.5 *Demodulation Application of Convolution*, 729
- A.6 Tables of Fourier Transforms and Operations, 731
- References, 732

B FUNDAMENTALS OF STATISTICAL DECISION THEORY

733

- B.1 Bayes' Theorem, 733
 - B.1.1 *Discrete Form of Bayes' Theorem*, 734
 - B.1.2 *Mixed Form of Bayes' Theorem*, 736

B.2	Decision Theory, 738
B.2.1	<i>Components of the Decision Theory Problem, 738</i>
B.2.2	<i>The Likelihood Ratio Test and the Maximum A Posteriori Criterion, 739</i>
B.2.3	<i>The Maximum Likelihood Criterion, 739</i>
B.3	Signal Detection Example, 740
B.3.1	<i>The Maximum Likelihood Binary Decision, 740</i>
B.3.2	<i>Probability of Bit Error, 741</i>
	References, 743

C	RESPONSE OF CORRELATORS TO WHITE NOISE	744
D	OFTEN USED IDENTITIES	746
E	A CONVOLUTIONAL ENCODER/DECODER COMPUTER PROGRAM	748
F	LIST OF SYMBOLS	759
	INDEX	765