
Contents

PREFACE

xvii

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*, 11
 - 1.1.4 *Digital versus Analog Performance Criteria*, 13
- 1.2 Classification of Signals, 14
 - 1.2.1 *Deterministic and Random Signals*, 14
 - 1.2.2 *Periodic and Nonperiodic Signals*, 14
 - 1.2.3 *Analog and Discrete Signals*, 14
 - 1.2.4 *Energy and Power Signals*, 14
 - 1.2.5 *The Unit Impulse Function*, 16
- 1.3 Spectral Density, 16
 - 1.3.1 *Energy Spectral Density*, 17
 - 1.3.2 *Power Spectral Density*, 17
- 1.4 Autocorrelation, 19
 - 1.4.1 *Autocorrelation of an Energy Signal*, 19
 - 1.4.2 *Autocorrelation of a Periodic (Power) Signal*, 20
- 1.5 Random Signals, 20
 - 1.5.1 *Random Variables*, 20
 - 1.5.2 *Random Processes*, 22
 - 1.5.3 *Time Averaging and Ergodicity*, 25
 - 1.5.4 *Power Spectral Density of a Random Process*, 26
 - 1.5.5 *Noise in Communication Systems*, 30

- 1.6 Signal Transmission through Linear Systems, 33
 - 1.6.1 Impulse Response, 34
 - 1.6.2 Frequency Transfer Function, 35
 - 1.6.3 Distortionless Transmission, 36
 - 1.6.4 Signals, Circuits, and Spectra, 42
- 1.7 Bandwidth of Digital Data, 45
 - 1.7.1 Baseband versus Bandpass, 45
 - 1.7.2 The Bandwidth Dilemma, 47
- 1.8 Conclusion, 51

2 FORMATTING AND BASEBAND MODULATION

55

- 2.1 Baseband Systems, 56
- 2.2 Formatting Textual Data (Character Coding), 58
- 2.3 Messages, Characters, and Symbols, 61
 - 2.3.1 Example of Messages, Characters, and Symbols, 61
- 2.4 Formatting Analog Information, 62
 - 2.4.1 The Sampling Theorem, 63
 - 2.4.2 Aliasing, 69
 - 2.4.3 Why Oversample? 72
 - 2.4.4 Signal Interface for a Digital System, 75
- 2.5 Sources of Corruption, 76
 - 2.5.1 Sampling and Quantizing Effects, 76
 - 2.5.2 Channel Effects, 77
 - 2.5.3 Signal-to-Noise Ratio for Quantized Pulses, 78
- 2.6 Pulse Code Modulation, 79
- 2.7 Uniform and Nonuniform Quantization, 81
 - 2.7.1 Statistics of Speech Amplitudes, 81
 - 2.7.2 Nonuniform Quantization, 83
 - 2.7.3 Companding Characteristics, 84
- 2.8 Baseband Modulation, 85
 - 2.8.1 Waveform Representation of Binary Digits, 85
 - 2.8.2 PCM Waveform Types, 85
 - 2.8.3 Spectral Attributes of PCM Waveforms, 89
 - 2.8.4 Bits per PCM Word and Bits per Symbol, 90
 - 2.8.5 M-ary Pulse Modulation Waveforms, 91
- 2.9 Correlative Coding, 94
 - 2.9.1 Duobinary Signaling, 94
 - 2.9.2 Duobinary Decoding, 95
 - 2.9.3 Precoding, 96
 - 2.9.4 Duobinary Equivalent Transfer Function, 97
 - 2.9.5 Comparison of Binary with Duobinary Signaling, 98
 - 2.9.6 Polybinary Signaling, 99
- 2.10 Conclusion, 100

3 BASEBAND DEMODULATION/DETECTION

104

- 3.1 Signals and Noise, 106
 - 3.1.1 Error-Performance Degradation in Communication Systems, 106
 - 3.1.2 Demodulation and Detection, 107
 - 3.1.3 A Vectorial View of Signals and Noise, 110
 - 3.1.4 The Basic SNR Parameter for Digital Communication Systems, 117
 - 3.1.5 Why E_b/N_0 Is a Natural Figure of Merit, 118
- 3.2 Detection of Binary Signals in Gaussian Noise, 119
 - 3.2.1 Maximum Likelihood Receiver Structure, 119
 - 3.2.2 The Matched Filter, 122
 - 3.2.3 Correlation Realization of the Matched Filter, 124
 - 3.2.4 Optimizing Error Performance, 127
 - 3.2.5 Error Probability Performance of Binary Signaling, 131
- 3.3 Intersymbol Interference, 136
 - 3.3.1 Pulse Shaping to Reduce ISI, 138
 - 3.3.2 Two Types of Error-Performance Degradation, 142
 - 3.3.3 Demodulation/Detection of Shaped Pulses, 145
- 3.4 Equalization, 149
 - 3.4.1 Channel Characterization, 149
 - 3.4.2 Eye Pattern, 151
 - 3.4.3 Equalizer Filter Types, 152
 - 3.4.4 Preset and Adaptive Equalization, 158
 - 3.4.5 Filter Update Rate, 160
- 3.5 Conclusion, 161

4 BANDPASS MODULATION AND DEMODULATION/DETECTION

167

- 4.1 Why Modulate? 168
- 4.2 Digital Bandpass Modulation Techniques, 169
 - 4.2.1 Phasor Representation of a Sinusoid, 171
 - 4.2.2 Phase Shift Keying, 173
 - 4.2.3 Frequency Shift Keying, 175
 - 4.2.4 Amplitude Shift Keying, 175
 - 4.2.5 Amplitude Phase Keying, 176
 - 4.2.6 Waveform Amplitude Coefficient, 176
- 4.3 Detection of Signals in Gaussian Noise, 177
 - 4.3.1 Decision Regions, 177
 - 4.3.2 Correlation Receiver, 178
- 4.4 Coherent Detection, 183
 - 4.4.1 Coherent Detection of PSK, 183
 - 4.4.2 Sampled Matched Filter, 184
 - 4.4.3 Coherent Detection of Multiple Phase Shift Keying, 188
 - 4.4.4 Coherent Detection of FSK, 191

- 4.5 Noncoherent Detection, 194
 - 4.5.1 *Detection of Differential PSK*, 194
 - 4.5.2 *Binary Differential PSK Example*, 196
 - 4.5.3 *Noncoherent Detection of FSK*, 198
 - 4.5.4 *Required Tone Spacing for Noncoherent Orthogonal FSK*, 200
- 4.6 Complex Envelope, 204
 - 4.6.1 *Quadrature Implementation of a Modulator*, 205
 - 4.6.2 *D8PSK Modulator Example*, 206
 - 4.6.3 *D8PSK Demodulator Example*, 208
- 4.7 Error Performance for Binary Systems, 209
 - 4.7.1 *Probability of Bit Error for Coherently Detected BPSK*, 209
 - 4.7.2 *Probability of Bit Error for Coherently Detected Differentially Encoded Binary PSK*, 211
 - 4.7.3 *Probability of Bit Error for Coherently Detected Binary Orthogonal FSK*, 213
 - 4.7.4 *Probability of Bit Error for Noncoherently Detected Binary Orthogonal FSK*, 213
 - 4.7.5 *Probability of Bit Error for Binary DPSK*, 216
 - 4.7.6 *Comparison of Bit Error Performance for Various Modulation Types*, 218
- 4.8 M-ary Signaling and Performance, 219
 - 4.8.1 *Ideal Probability of Bit Error Performance*, 219
 - 4.8.2 *M-ary Signaling*, 220
 - 4.8.3 *Vectorial View of MPSK Signaling*, 222
 - 4.8.4 *BPSK and QPSK Have the Same Bit Error Probability*, 223
 - 4.8.5 *Vectorial View of MFSK Signaling*, 225
- 4.9 Symbol Error Performance for M-ary Systems ($M > 2$), 229
 - 4.9.1 *Probability of Symbol Error for MPSK*, 229
 - 4.9.2 *Probability of Symbol Error for MFSK*, 230
 - 4.9.3 *Bit Error Probability versus Symbol Error Probability for Orthogonal Signals*, 232
 - 4.9.4 *Bit Error Probability versus Symbol Error Probability for Multiple Phase Signaling*, 234
 - 4.9.5 *Effects of Intersymbol Interference*, 235
- 4.10 Conclusion, 236

5 COMMUNICATIONS LINK ANALYSIS

242

- 5.1 What the System Link Budget Tells the System Engineer, 243
- 5.2 The Channel, 244
 - 5.2.1 *The Concept of Free Space*, 244
 - 5.2.2 *Error-Performance Degradation*, 245
 - 5.2.3 *Sources of Signal Loss and Noise*, 245

- 5.3 Received Signal Power and Noise Power, 250
 - 5.3.1 *The Range Equation*, 250
 - 5.3.2 *Received Signal Power as a Function of Frequency*, 254
 - 5.3.3 *Path Loss is Frequency Dependent*, 256
 - 5.3.4 *Thermal Noise Power*, 258
- 5.4 Link Budget Analysis, 259
 - 5.4.1 *Two E_b/N_0 Values of Interest*, 262
 - 5.4.2 *Link Budgets are Typically Calculated in Decibels*, 263
 - 5.4.3 *How Much Link Margin is Enough?* 264
 - 5.4.4 *Link Availability*, 266
- 5.5 Noise Figure, Noise Temperature, and System Temperature, 270
 - 5.5.1 *Noise Figure*, 270
 - 5.5.2 *Noise Temperature*, 273
 - 5.5.3 *Line Loss*, 274
 - 5.5.4 *Composite Noise Figure and Composite Noise Temperature*, 276
 - 5.5.5 *System Effective Temperature*, 277
 - 5.5.6 *Sky Noise Temperature*, 282
- 5.6 Sample Link Analysis, 286
 - 5.6.1 *Link Budget Details*, 287
 - 5.6.2 *Receiver Figure of Merit*, 289
 - 5.6.3 *Received Isotropic Power*, 289
- 5.7 Satellite Repeaters, 290
 - 5.7.1 *Nonregenerative Repeaters*, 291
 - 5.7.2 *Nonlinear Repeater Amplifiers*, 295
- 5.8 System Trade-Offs, 296
- 5.9 Conclusion, 297

6 CHANNEL CODING: PART 1

304

- 6.1 Waveform Coding and Structured Sequences, 305
 - 6.1.1 *Antipodal and Orthogonal Signals*, 307
 - 6.1.2 *M-ary Signaling*, 308
 - 6.1.3 *Waveform Coding*, 309
 - 6.1.4 *Waveform-Coding System Example*, 313
- 6.2 Types of Error Control, 315
 - 6.2.1 *Terminal Connectivity*, 315
 - 6.2.2 *Automatic Repeat Request*, 316
- 6.3 Structured Sequences, 317
 - 6.3.1 *Channel Models*, 318
 - 6.3.2 *Code Rate and Redundancy*, 320
 - 6.3.3 *Parity Check Codes*, 321
 - 6.3.4 *Why Use Error-Correction Coding?* 323

- 6.4 Linear Block Codes, 328
 - 6.4.1 Vector Spaces, 329
 - 6.4.2 Vector Subspaces, 329
 - 6.4.3 A (6, 3) Linear Block Code Example, 330
 - 6.4.4 Generator Matrix, 331
 - 6.4.5 Systematic Linear Block Codes, 333
 - 6.4.6 Parity-Check Matrix, 334
 - 6.4.7 Syndrome Testing, 335
 - 6.4.8 Error Correction, 336
 - 6.4.9 Decoder Implementation, 340
- 6.5 Error-Detecting and Correcting Capability, 342
 - 6.5.1 Weight and Distance of Binary Vectors, 342
 - 6.5.2 Minimum Distance of a Linear Code, 343
 - 6.5.3 Error Detection and Correction, 343
 - 6.5.4 Visualization of a 6-Tuple Space, 347
 - 6.5.5 Erasure Correction, 348
- 6.6 Usefulness of the Standard Array, 349
 - 6.6.1 Estimating Code Capability, 349
 - 6.6.2 An (n, k) Example, 351
 - 6.6.3 Designing the $(8, 2)$ Code, 352
 - 6.6.4 Error Detection versus Error Correction Trade-Offs, 352
 - 6.6.5 The Standard Array Provides Insight, 356
- 6.7 Cyclic Codes, 356
 - 6.7.1 Algebraic Structure of Cyclic Codes, 357
 - 6.7.2 Binary Cyclic Code Properties, 358
 - 6.7.3 Encoding in Systematic Form, 359
 - 6.7.4 Circuit for Dividing Polynomials, 360
 - 6.7.5 Systematic Encoding with an $(n - k)$ -Stage Shift Register, 363
 - 6.7.6 Error Detection with an $(n - k)$ -Stage Shift Register, 365
- 6.8 Well-Known Block Codes, 366
 - 6.8.1 Hamming Codes, 366
 - 6.8.2 Extended Golay Code, 369
 - 6.8.3 BCH Codes, 370
- 6.9 Conclusion, 374

7 CHANNEL CODING: PART 2

381

- 7.1 Convolutional Encoding, 382
- 7.2 Convolutional Encoder Representation, 384
 - 7.2.1 Connection Representation, 385
 - 7.2.2 State Representation and the State Diagram, 389
 - 7.2.3 The Tree Diagram, 391
 - 7.2.4 The Trellis Diagram, 393
- 7.3 Formulation of the Convolutional Decoding Problem, 395
 - 7.3.1 Maximum Likelihood Decoding, 395

- 7.3.2 Channel Models: Hard versus Soft Decisions, 396
- 7.3.3 The Viterbi Convolutional Decoding Algorithm, 401
- 7.3.4 An Example of Viterbi Convolutional Decoding, 401
- 7.3.5 Decoder Implementation, 405
- 7.3.6 Path Memory and Synchronization, 408
- 7.4 Properties of Convolutional Codes, 408
 - 7.4.1 Distance Properties of Convolutional Codes, 408
 - 7.4.2 Systematic and Nonsystematic Convolutional Codes, 413
 - 7.4.3 Catastrophic Error Propagation in Convolutional Codes, 414
 - 7.4.4 Performance Bounds for Convolutional Codes, 415
 - 7.4.5 Coding Gain, 416
 - 7.4.6 Best Known Convolutional Codes, 418
 - 7.4.7 Convolutional Code Rate Trade-Off, 420
 - 7.4.8 Soft-Decision Viterbi Decoding, 420
- 7.5 Other Convolutional Decoding Algorithms, 422
 - 7.5.1 Sequential Decoding, 422
 - 7.5.2 Comparisons and Limitations of Viterbi and Sequential Decoding, 425
 - 7.5.3 Feedback Decoding, 427
- 7.6 Conclusion, 429

8 CHANNEL CODING: PART 3

436

- 8.1 Reed-Solomon Codes, 437
 - 8.1.1 Reed-Solomon Error Probability, 438
 - 8.1.2 Why R-S Codes Perform Well Against Burst Noise, 441
 - 8.1.3 R-S Performance as a Function of Size, Redundancy, and Code Rate, 441
 - 8.1.4 Finite Fields, 445
 - 8.1.5 Reed-Solomon Encoding, 450
 - 8.1.6 Reed-Solomon Decoding, 454
- 8.2 Interleaving and Concatenated Codes, 461
 - 8.2.1 Block Interleaving, 463
 - 8.2.2 Convolutional Interleaving, 466
 - 8.2.3 Concatenated Codes, 468
- 8.3 Coding and Interleaving Applied to the Compact Disc Digital Audio System, 469
 - 8.3.1 CIRC Encoding, 470
 - 8.3.2 CIRC Decoding, 472
 - 8.3.3 Interpolation and Muting, 474
- 8.4 Turbo Codes, 475
 - 8.4.1 Turbo Code Concepts, 477
 - 8.4.2 Log-Likelihood Algebra, 481
 - 8.4.3 Product Code Example, 482
 - 8.4.4 Encoding with Recursive Systematic Codes, 488
 - 8.4.5 A Feedback Decoder, 493

- 8.4.6 *The MAP Decoding Algorithm*, 498
- 8.4.7 *MAP Decoding Example*, 504
- 8.5 Conclusion, 509
- Appendix 8A The Sum of Log-Likelihood Ratios, 510

9 MODULATION AND CODING TRADE-OFFS 520

- 9.1 Goals of the Communications System Designer, 521
- 9.2 Error Probability Plane, 522
- 9.3 Nyquist Minimum Bandwidth, 524
- 9.4 Shannon-Hartley Capacity Theorem, 525
 - 9.4.1 *Shannon Limit*, 528
 - 9.4.2 *Entropy*, 529
 - 9.4.3 *Equivocation and Effective Transmission Rate*, 532
- 9.5 Bandwidth Efficiency Plane, 534
 - 9.5.1 *Bandwidth Efficiency of MPSK and MFSK Modulation*, 535
 - 9.5.2 *Analogies Between Bandwidth-Efficiency and Error Probability Planes*, 536
- 9.6 Modulation and Coding Trade-Offs, 537
- 9.7 Defining, Designing, and Evaluating Digital Communication Systems, 538
 - 9.7.1 *M-ary Signaling*, 539
 - 9.7.2 *Bandwidth-Limited Systems*, 540
 - 9.7.3 *Power-Limited Systems*, 541
 - 9.7.4 *Requirements for MPSK and MFSK Signaling*, 542
 - 9.7.5 *Bandwidth-Limited Uncoded System Example*, 543
 - 9.7.6 *Power-Limited Uncoded System Example*, 545
 - 9.7.7 *Bandwidth-Limited and Power-Limited Coded System Example*, 547
- 9.8 Bandwidth-Efficient Modulation, 555
 - 9.8.1 *QPSK and Offset QPSK Signaling*, 555
 - 9.8.2 *Minimum Shift Keying*, 559
 - 9.8.3 *Quadrature Amplitude Modulation*, 563
- 9.9 Modulation and Coding for Bandlimited Channels, 566
 - 9.9.1 *Commercial Telephone Modems*, 567
 - 9.9.2 *Signal Constellation Boundaries*, 568
 - 9.9.3 *Higher Dimensional Signal Constellations*, 569
 - 9.9.4 *Higher-Density Lattice Structures*, 572
 - 9.9.5 *Combined Gain: N-Sphere Mapping and Dense Lattice*, 573
- 9.10 Trellis-Coded Modulation, 573
 - 9.10.1 *The Idea Behind Trellis-Coded Modulation (TCM)*, 574
 - 9.10.2 *TCM Encoding*, 576
 - 9.10.3 *TCM Decoding*, 580
 - 9.10.4 *Other Trellis Codes*, 583

- 9.10.5 *Trellis-Coded Modulation Example*, 585
- 9.10.6 *Multi-Dimensional Trellis-Coded Modulation*, 589
- 9.11 Conclusion, 590

10 SYNCHRONIZATION 598

- 10.1 Introduction, 599
 - 10.1.1 *Synchronization Defined*, 599
 - 10.1.2 *Costs versus Benefits*, 601
 - 10.1.3 *Approach and Assumptions*, 602
- 10.2 Receiver Synchronization, 603
 - 10.2.1 *Frequency and Phase Synchronization*, 603
 - 10.2.2 *Symbol Synchronization—Discrete Symbol Modulations*, 625
 - 10.2.3 *Synchronization with Continuous-Phase Modulations (CPM)*, 631
 - 10.2.4 *Frame Synchronization*, 639
- 10.3 Network Synchronization, 643
 - 10.3.1 *Open-Loop Transmitter Synchronization*, 644
 - 10.3.2 *Closed-Loop Transmitter Synchronization*, 647
- 10.4 Conclusion, 649

11 MULTIPLEXING AND MULTIPLE ACCESS 656

- 11.1 Allocation of the Communications Resource, 657
 - 11.1.1 *Frequency-Division Multiplexing/Multiple Access*, 660
 - 11.1.2 *Time-Division Multiplexing/Multiple Access*, 665
 - 11.1.3 *Communications Resource Channelization*, 668
 - 11.1.4 *Performance Comparison of FDMA and TDMA*, 668
 - 11.1.5 *Code-Division Multiple Access*, 672
 - 11.1.6 *Space-Division and Polarization-Division Multiple Access*, 674
- 11.2 Multiple Access Communications System and Architecture, 676
 - 11.2.1 *Multiple Access Information Flow*, 677
 - 11.2.2 *Demand Assignment Multiple Access*, 678
- 11.3 Access Algorithms, 678
 - 11.3.1 *ALOHA*, 678
 - 11.3.2 *Slotted ALOHA*, 682
 - 11.3.3 *Reservation-ALOHA*, 683
 - 11.3.4 *Performance Comparison of S-ALOHA and R-ALOHA*, 684
 - 11.3.5 *Polling Techniques*, 686
- 11.4 Multiple Access Techniques Employed with INTELSAT, 689
 - 11.4.1 *Preassigned FDM/FM/FDMA or MCPC Operation*, 690
 - 11.4.2 *MCPC Modes of Accessing an INTELSAT Satellite*, 690
 - 11.4.3 *SPADE Operation*, 693
 - 11.4.4 *TDMA in INTELSAT*, 698
 - 11.4.5 *Satellite-Switched TDMA in INTELSAT*, 704

- 11.5 Multiple Access Techniques for Local Area Networks, 708
 - 11.5.1 Carrier-Sense Multiple Access Networks, 708
 - 11.5.2 Token-Ring Networks, 710
 - 11.5.3 Performance Comparison of CSMA/CD and Token-Ring Networks, 711
- 11.6 Conclusion, 713

12 SPREAD-SPECTRUM TECHNIQUES

718

- 12.1 Spread-Spectrum Overview, 719
 - 12.1.1 The Beneficial Attributes of Spread-Spectrum Systems, 720
 - 12.1.2 A Catalog of Spreading Techniques, 724
 - 12.1.3 Model for Direct-Sequence Spread-Spectrum Interference Rejection, 726
 - 12.1.4 Historical Background, 727
- 12.2 Pseudonoise Sequences, 728
 - 12.2.1 Randomness Properties, 729
 - 12.2.2 Shift Register Sequences, 729
 - 12.2.3 PN Autocorrelation Function, 730
- 12.3 Direct-Sequence Spread-Spectrum Systems, 732
 - 12.3.1 Example of Direct Sequencing, 734
 - 12.3.2 Processing Gain and Performance, 735
- 12.4 Frequency Hopping Systems, 738
 - 12.4.1 Frequency Hopping Example, 740
 - 12.4.2 Robustness, 741
 - 12.4.3 Frequency Hopping with Diversity, 741
 - 12.4.4 Fast Hopping versus Slow Hopping, 742
 - 12.4.5 FFH/MFSK Demodulator, 744
 - 12.4.6 Processing Gain, 745
- 12.5 Synchronization, 745
 - 12.5.1 Acquisition, 746
 - 12.5.2 Tracking, 751
- 12.6 Jamming Considerations, 754
 - 12.6.1 The Jamming Game, 754
 - 12.6.2 Broadband Noise Jamming, 759
 - 12.6.3 Partial-Band Noise Jamming, 760
 - 12.6.4 Multiple-Tone Jamming, 763
 - 12.6.5 Pulse Jamming, 763
 - 12.6.6 Repeat-Back Jamming, 765
 - 12.6.7 BLADES System, 768
- 12.7 Commercial Applications, 769
 - 12.7.1 Code-Division Multiple Access, 769
 - 12.7.2 Multipath Channels, 771
 - 12.7.3 The FCC Part 15 Rules for Spread-Spectrum Systems, 772
 - 12.7.4 Direct Sequence versus Frequency Hopping, 773
- 12.8 Cellular Systems, 775
 - 12.8.1 Direct Sequence CDMA, 776

xiv

Contents

- 12.8.2 Analog FM versus TDMA versus CDMA, 779
- 12.8.3 Interference-Limited versus Dimension-Limited Systems, 781
- 12.8.4 IS-95 CDMA Digital Cellular System, 782
- 12.9 Conclusion, 795

13 SOURCE CODING

803

- 13.1 Sources, 804
 - 13.1.1 Discrete Sources, 804
 - 13.1.2 Waveform Sources, 809
- 13.2 Amplitude Quantizing, 811
 - 13.2.1 Quantizing Noise, 813
 - 13.2.2 Uniform Quantizing, 816
 - 13.2.3 Saturation, 820
 - 13.2.4 Dithering, 823
 - 13.2.5 Nonuniform Quantizing, 826
- 13.3 Differential Pulse-Code Modulation, 835
 - 13.3.1 One-Tap Prediction, 838
 - 13.3.2 N-Tap Prediction, 839
 - 13.3.3 Delta Modulation, 841
 - 13.3.4 Sigma-Delta Modulation, 842
 - 13.3.5 Sigma-Delta A-to-D Converter (ADC), 847
 - 13.3.6 Sigma-Delta D-to-A Converter (DAC), 848
- 13.4 Adaptive Prediction, 850
 - 13.4.1 Forward Prediction, 851
 - 13.4.2 Synthesis/Analysis Coding, 852
- 13.5 Block Coding, 853
 - 13.5.1 Vector Quantizing, 854
- 13.6 Transform Coding, 856
 - 13.6.1 Quantization for Transform Coding, 857
 - 13.6.2 Subband Coding, 857
- 13.7 Source Coding for Digital Data, 859
 - 13.7.1 Properties of Codes, 860
 - 13.7.2 Huffman Codes, 862
 - 13.7.3 Run-Length Codes, 866
- 13.8 Examples of Source Coding, 870
 - 13.8.1 Audio Compression, 870
 - 13.8.2 Image Compression, 875
- 13.9 Conclusion, 884

14 ENCRYPTION AND DECRYPTION

890

- 14.1 Models, Goals, and Early Cipher Systems, 891
 - 14.1.1 A Model of the Encryption and Decryption Process, 893
 - 14.1.2 System Goals, 893
 - 14.1.3 Classic Threats, 893

Contents

xv

- 14.1.4 *Classic Ciphers*, 894
- 14.2 The Secrecy of a Cipher System, 897
 - 14.2.1 *Perfect Secrecy*, 897
 - 14.2.2 *Entropy and Equivocation*, 900
 - 14.2.3 *Rate of a Language and Redundancy*, 902
 - 14.2.4 *Unicity Distance and Ideal Secrecy*, 902
- 14.3 Practical Security, 905
 - 14.3.1 *Confusion and Diffusion*, 905
 - 14.3.2 *Substitution*, 905
 - 14.3.3 *Permutation*, 907
 - 14.3.4 *Product Cipher Systems*, 908
 - 14.3.5 *The Data Encryption Standard*, 909
- 14.4 Stream Encryption, 915
 - 14.4.1 *Example of Key Generation Using a Linear Feedback Shift Register*, 916
 - 14.4.2 *Vulnerabilities of Linear Feedback Shift Registers*, 917
 - 14.4.3 *Synchronous and Self-Synchronous Stream Encryption Systems*, 919
- 14.5 Public Key Cryptosystems, 920
 - 14.5.1 *Signature Authentication using a Public Key Cryptosystem*, 921
 - 14.5.2 *A Trapdoor One-Way Function*, 922
 - 14.5.3 *The Rivest-Shamir-Adelman Scheme*, 923
 - 14.5.4 *The Knapsack Problem*, 925
 - 14.5.5 *A Public Key Cryptosystem based on a Trapdoor Knapsack*, 927
- 14.6 Pretty Good Privacy, 929
 - 14.6.1 *Triple-DES, CAST, and IDEA*, 931
 - 14.6.2 *Diffie-Hellman (Elgamal Variation) and RSA*, 935
 - 14.6.3 *PGP Message Encryption*, 936
 - 14.6.4 *PGP Authentication and Signature*, 937
- 14.7 Conclusion, 940

15 FADING CHANNELS

944

- 15.1 The Challenge of Communicating over Fading Channels, 945
- 15.2 Characterizing Mobile-Radio Propagation, 947
 - 15.2.1 *Large-Scale Fading*, 951
 - 15.2.2 *Small-Scale Fading*, 953
- 15.3 Signal Time-Spreading, 958
 - 15.3.1 *Signal Time-Spreading Viewed in the Time-Delay Domain*, 958
 - 15.3.2 *Signal Time-Spreading Viewed in the Frequency Domain*, 960
 - 15.3.3 *Examples of Flat Fading and Frequency-Selective Fading*, 965
- 15.4 Time Variance of the Channel Caused by Motion, 966
 - 15.4.1 *Time Variance Viewed in the Time Domain*, 966
 - 15.4.2 *Time Variance Viewed in the Doppler-Shift Domain*, 969
 - 15.4.3 *Performance over a Slow- and Flat-Fading Rayleigh Channel*, 975

- 15.5 Mitigating the Degradation Effects of Fading, 978
 - 15.5.1 *Mitigation to Combat Frequency-Selective Distortion*, 980
 - 15.5.2 *Mitigation to Combat Fast-Fading Distortion*, 982
 - 15.5.3 *Mitigation to Combat Loss in SNR*, 983
 - 15.5.4 *Diversity Techniques*, 984
 - 15.5.5 *Modulation Types for Fading Channels*, 987
 - 15.5.6 *The Role of an Interleaver*, 988
- 15.6 Summary of the Key Parameters Characterizing Fading Channels, 992
 - 15.6.1 *Fast Fading Distortion: Case 1*, 992
 - 15.6.2 *Frequency-Selective Fading Distortion: Case 2*, 993
 - 15.6.3 *Fast-Fading and Frequency-Selective Fading Distortion: Case 3*, 993
- 15.7 Applications: Mitigating the Effects of Frequency-Selective Fading, 996
 - 15.7.1 *The Viterbi Equalizer as Applied to GSM*, 996
 - 15.7.2 *The Rake Receiver as Applied to Direct-Sequence Spread-Spectrum (DS/SS) Systems*, 999
- 15.8 Conclusion, 1001

A A REVIEW OF FOURIER TECHNIQUES

1012

- A.1 Signals, Spectra, and Linear Systems, 1012
- A.2 Fourier Techniques for Linear System Analysis, 1012
 - A.2.1 *Fourier Series Transform*, 1014
 - A.2.2 *Spectrum of a Pulse Train*, 1018
 - A.2.3 *Fourier Integral Transform*, 1020
- A.3 Fourier Transform Properties, 1021
 - A.3.1 *Time Shifting Property*, 1022
 - A.3.2 *Frequency Shifting Property*, 1022
- A.4 Useful Functions, 1023
 - A.4.1 *Unit Impulse Function*, 1023
 - A.4.2 *Spectrum of a Sinusoid*, 1023
- A.5 Convolution, 1025
 - A.5.1 *Graphical Example of Convolution*, 1027
 - A.5.2 *Time Convolution Property*, 1028
 - A.5.3 *Frequency Convolution Property*, 1030
 - A.5.4 *Convolution of a Function with a Unit Impulse*, 1030
 - A.5.5 *Demodulation Application of Convolution*, 1031
- A.6 Tables of Fourier Transforms and Operations, 1033

B FUNDAMENTALS OF STATISTICAL DECISION THEORY 1035

- B.1 Bayes' Theorem, 1035
 - B.1.1 *Discrete Form of Bayes' Theorem*, 1036
 - B.1.2 *Mixed Form of Bayes' Theorem*, 1038
- B.2 Decision Theory, 1040
 - B.2.1 *Components of the Decision Theory Problem*, 1040

B.2.2	<i>The Likelihood Ratio Test and the Maximum A Posteriori Criterion,</i>	1041
B.2.3	<i>The Maximum Likelihood Criterion,</i>	1042
B.3	Signal Detection Example,	1042
B.3.1	<i>The Maximum Likelihood Binary Decision,</i>	1042
B.3.2	<i>Probability of Bit Error,</i>	1044
C	RESPONSE OF A CORRELATOR TO WHITE NOISE	1047
D	OFTEN-USED IDENTITIES	1049
E	s-DOMAIN, z-DOMAIN AND DIGITAL FILTERING	1051
E.1	The Laplace Transform,	1051
E.1.1	<i>Standard Laplace Transforms,</i>	1052
E.1.2	<i>Laplace Transform Properties,</i>	1053
E.1.3	<i>Using the Laplace Transform,</i>	1054
E.1.4	<i>Transfer Function,</i>	1055
E.1.5	<i>RC Circuit Low Pass Filtering,</i>	1056
E.1.6	<i>Poles and Zeroes,</i>	1056
E.1.7	<i>Linear System Stability,</i>	1057
E.2	The z-Transform,	1058
E.2.1	<i>Calculating the z-Transform,</i>	1058
E.2.2	<i>The Inverse z-Transform,</i>	1059
E.3	Digital Filtering,	1060
E.3.1	<i>Digital Filter Transfer Function,</i>	1061
E.3.2	<i>Single Pole Filter Stability,</i>	1062
E.3.3	<i>General Digital Filter Stability,</i>	1063
E.3.4	<i>z-Plane Pole-Zero Diagram and the Unit Circle,</i>	1063
E.3.5	<i>Discrete Fourier Transform of Digital Filter Impulse Response,</i>	1064
E.4	Finite Impulse Response Filter Design,	1065
E.4.1	<i>FIR Filter Design,</i>	1065
E.4.2	<i>The FIR Differentiator,</i>	1067
E.5	Infinite Impulse Response Filter Design,	1069
E.5.1	<i>Backward Difference Operator,</i>	1069
E.5.2	<i>IIR Filter Design using the Bilinear Transform,</i>	1070
E.5.3	<i>The IIR Integrator,</i>	1071
F	LIST OF SYMBOLS	1072
	INDEX	1074