Basics of communications and coding

William G. Chambers

Department of Electronic and Electrical Engineering,
King's College London (KQC)
Contents

Glossary of function names and symbols xv

1 Introduction 1
  1.1 Aims and outline 1
    1.1.1 Introductory comments 1
    1.1.2 Communications 1
    1.1.3 The robustness of digital communications 2
    1.1.4 Reliable communications 3
    1.1.5 Outline 4
  1.2 Physical background 6
    1.2.1 Frequency bands 6
    1.2.2 Power and power flux 8
    1.2.3 The decibel 9
    1.2.4 Noise and interference 10

Exercises 11

2 Fourier theory 13
  2.1 The Fourier transform 13
    2.1.1 The Fourier inversion theorem 13
    2.1.2 A few simple results 16
    2.1.3 Convolutions and correlations 17
  2.2 The delta function 19
    2.2.1 Definition and properties 19
    2.2.2 The Fourier transform 20
    2.2.3 Filters 20
    2.2.4 Impulse response function 21
    2.2.5 Transfer function 22
    2.2.6 Some examples of filters 23
  2.3 Periodic functions 26
    2.3.1 Fourier series 26
    2.3.2 A few simple results 29
    2.3.3 Filtering a periodic function 30
    2.3.4 Periodically repeated functions 32
    2.3.5 The looped wave-guide 32
  2.4 Delta combs 34
    2.4.1 Fourier transform of a periodic function 34
    2.4.2 The periodic comb 34

Exercises 36
3 Digital signalling methods

3.1 The concept of information
   3.1.1 Information and information rates
   3.1.2 Data compression

3.2 Baseband signalling
   3.2.1 Baseband binary and multilevel pulse signalling
   3.2.2 Information rate for 'moderate reliability'
   3.2.3 Gray codes
   3.2.4 Codes and signals
   3.2.5 Nyquist sampling of analogue signals
   3.2.6 Analogue-to-digital conversion
   3.2.7 Links using repeaters

3.3 Band-restricted signalling
   3.3.1 Band-restricted pulse signalling
   3.3.2 Intersymbol interference
   3.3.3 Adaptive equalizers
   3.3.4 Duobinary system

3.4 Carrier-based signalling
   3.4.1 Carrier modulation
   3.4.2 Positive-frequency and phasor representations
   3.4.3 Quadrature modulation
   3.4.4 Carrier-based pulse signalling
   3.4.5 Frequency-shift keying

Exercises

4 Random variables and noise

4.1 Probability theory
   4.1.1 Basic concepts
   4.1.2 Random variables
   4.1.3 Continuous random variables
   4.1.4 The Chernoff bound
   4.1.5 Gaussian distributions
   4.1.6 Multivariate Gaussian distributions

4.2 Noise signals
   4.2.1 Introductory
   4.2.2 The autocorrelation function
   4.2.3 The effect of filtering on noise
   4.2.4 White noise
CONTENTS

4.2.5 Shot noise 82
4.2.6 Gaussian noise 85

4.3 Gaussian noise in polar signalling 86
  4.3.1 Introductory 86
  4.3.2 Integrating a single pulse 86
  4.3.3 Error probability 87
  4.3.4 Reliable communication 87

4.4 Rayleigh fading 89
  4.4.1 Rayleigh channel 89
  4.4.2 Error probability 90

Exercises 91

5 Signal spaces 94

5.1 Expansions as function spaces 94
  5.1.1 Introductory 94
  5.1.2 Dimension and bandwidth equivalent 95
  5.1.3 Scalar product and length 96
  5.1.4 Expansions with an orthonormal basis 97
  5.1.5 Some examples of signal spaces 98
  5.1.6 Hadamard functions 99
  5.1.7 Matched filters 101
  5.1.8 The effect of additive white noise 102

5.2 Codes in signal-space 103
  5.2.1 Introductory 103
  5.2.2 Lattice codes 106
  5.2.3 Spherical codes 107
  5.2.4 Orthogonal and biorthogonal signalling 107

5.3 Shannon's theorem 111
  5.3.1 Introductory 111
  5.3.2 The theorem 111
  5.3.3 Random coding 114
  5.3.4 The converse theorem 114
  5.3.5 Reliability and complexity 114
  5.3.6 Wide-band and narrow-band signalling 115
  5.3.7 To code or not to code 116

Exercises 119
6 Error-correcting codes

6.1 Codes and channels

6.1.1 The BSC and binary codes
6.1.2 Feedback and forward error-correction
6.1.3 Simple codes on the AWGN channel
6.1.4 Burst channels

6.2 Trellis codes and the Viterbi algorithm

6.2.1 The duobinary code as a trellis code
6.2.2 The Viterbi algorithm
6.2.3 MSK modulation and multi-\(\phi\) phase codes
6.2.4 Convolutional codes

6.3 Binary linear block codes

6.3.1 Introductory
6.3.2 Binary hard-decision decoding
6.3.3 The parity-check matrix and the syndrome
6.3.4 Hamming codes
6.3.5 Two particular codes

6.4 Binary block codes on the AWGN channel

6.4.1 Binary linear codes on the AWGN channel
6.4.2 Performance of Reed-Muller codes
6.4.3 Weakness of hard-decision decoding
6.4.4 Hard-decision decoding with ARQ
6.4.5 Chase's soft-decision algorithm
6.4.6 Viterbi decoding of block codes

Exercises

7 Codes based on fields and polynomials

7.1 Fields

7.1.1 Modular arithmetic
7.1.2 Rings
7.1.3 Fields
7.1.4 Extensions and \(GF(2^m)\)

7.2 Hamming and BCH codes

7.2.1 Hamming codes
7.2.2 BCH codes

7.3 Polynomials

7.3.1 Polynomials and their degrees
7.3.2 Factors and multiples
7.3.3 Division algorithm
CONTENTS

7.3.4 The mod operation and congruences 162
7.3.5 Polynomial rings 163

7.4 Cyclic codes 163
7.4.1 Generator polynomial 163
7.4.2 Cyclic property 165

7.5 Reed–Solomon codes 167
7.5.1 The code 167
7.5.2 Check-sum conditions 168

7.6 Euclid’s algorithm 169
7.6.1 The algorithm 169
7.6.2 Some consequences 171
7.6.3 Properties of inverses mod \( G \) 173
7.6.4 Examples of inverses 173

7.7 Algebraic decoding 174
7.7.1 Introductory 174
7.7.2 The key equation 174
7.7.3 Euclidean algorithm 176
7.7.4 Erasures as well 176
7.7.5 Variations on a theme 177

7.8 Concatenated codes 178
7.8.1 Double encoding 178
7.8.2 Decoding complexity 180
7.8.3 Reliability 180

Exercises 182

8 Optical communications and quantum effects 184
8.1 Optical communications 184
8.1.1 Introductory 184
8.1.2 Optical fibres 185

8.2 Reception 187
8.2.1 The photo-electric effect 187
8.2.2 Photodetection followed by amplification 188
8.2.3 The ideal photodetector 189
8.2.4 PPM system 190
8.2.5 Coherent reception 192

8.3 Quantum theory 195
8.3.1 Photons in an ideal single-mode cavity 195
8.3.2 The suppression of thermal noise 196
CONTENTS

8.3.3 Maximum rate of transmission of information 197
8.3.4 More on photon counting 199
8.3.5 Comparisons with the upper bound 200

Exercises 201

9 Cipher systems 203
9.1 Introduction 203
  9.1.1 Basic terminology 203
  9.1.2 Monoalphabetic and bigram ciphers 204
  9.1.3 Running-key cipher 205
  9.1.4 Some further comments 205
  9.1.5 Functions and mappings 206
9.2 Conventional ciphers 207
  9.2.1 The one-time pad 207
  9.2.2 Theoretical secrecy 208
  9.2.3 Known-plaintext attack 210
9.3 Stream ciphers 211
  9.3.1 Introductory 211
  9.3.2 Feedback shift-registers 211
  9.3.3 The division algorithm revisited 212
  9.3.4 Introducing non-linearity 214
  9.3.5 Other problems 215
9.4 Block ciphers 216
  9.4.1 Affine transformations 216
  9.4.2 IBM systems 217
  9.4.3 Feistel cipher and the DES system 219
  9.4.4 Cipher feedback 220
9.5 Public key ciphers 221
  9.5.1 Public key-distribution 221
  9.5.2 RSA cipher 223

Exercises 226

Appendixes 228
  A Exact error probability for biorthogonal codes 228
  B Justification of the Euclidean algorithm 229

References 232

Index 236