

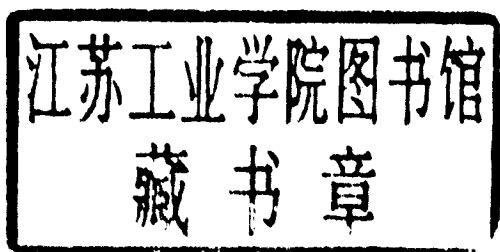
Mathematics for Engineers

Georges Fiche
G rard H buterne

ISTE

 WILEY

Mathematics for Engineers



Mathematics for Engineers

Georges Fiche
G rard H buterne

Series Editor
Pierre-No l Favennec

ISTE

 WILEY

First published in France in 2007 by Hermes Science/Lavoisier entitled: "Mathématiques pour les télécoms"

First published in Great Britain and the United States in 2008 by ISTE Ltd and John Wiley & Sons, Inc.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

© ISTE Ltd, 2008

© GET et LAVOISIER, 2007

The rights of Georges Fiche and Gérard Hébuterne to be identified as the authors of this work have been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

Library of Congress Cataloging-in-Publication Data

Fiche, Georges.

[Mathématiques pour les télécoms. English]

Mathematics for engineers / Georges Fiche, Gérard Hébuterne.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-84821-055-4 (talk. paper)

1. Engineering mathematics. I. Hébuterne, Gérard. II. Title.

TA330.F5313 2008

621.38201'51--dc22

2008030348

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library

ISBN: 978-1-84821-055-4

Cover image created by Atelier Isatis.

Printed and bound in Great Britain by CPI/Antony Rowe Ltd, Chippenham, Wiltshire.



Contents

Preface	15
Chapter 1. Probability Theory	19
1.1. Definition and properties of events	19
1.1.1. The concept of an event	19
1.1.2. Complementary events	21
1.1.2.1. Basic properties	21
1.1.3. Properties of operations on events	21
1.1.3.1. Commutativity	21
1.1.3.2. Associativity	21
1.1.3.3. Distributivity	21
1.1.3.4. Difference	21
1.1.3.5. De Morgan's rules	22
1.2. Probability	23
1.2.1. Definition	23
1.2.2. Basic theorems and results	23
1.2.2.1. Addition theorem	23
1.2.2.2. Conditional probability	24
1.2.2.3. Multiplication theorem	25
1.2.2.4. The posterior probability theorem	26
1.3. Random variable	27
1.3.1. Definition	27
1.3.2. Probability functions of a random variable	27
1.3.2.1. Notations	27
1.3.2.2. Cumulative distribution function	27
1.3.2.3. Probability density function	27
1.3.3. Moments of a random variable	28
1.3.3.1. Moments about the origin	29
1.3.3.2. Central moments	29

1.3.3.3. Mean and variance	29
1.3.3.4. Example applications	31
1.3.4. Couples of random variables	32
1.3.4.1. Definition	32
1.3.4.2. Joint probability	32
1.3.4.3. Marginal probability of couples of random variables	33
1.3.4.4. Conditional probability of a couple of random variables	34
1.3.4.5. Functions of a couple of random variables	34
1.3.4.6. Sum of independent random variables	36
1.3.4.7. Moments of the sum of independent random variables	37
1.3.4.8. Practical interest	39
1.4. Convolution	40
1.4.1. Definition	40
1.4.2. Properties of the convolution operation	41
1.4.2.1. The convolution is commutative	41
1.4.2.2. Convolution of exponential distributions	41
1.4.2.3. Convolution of normal (Gaussian) distributions	41
1.5. Laplace transform	42
1.5.1. Definition	43
1.5.2. Properties	43
1.5.2.1. Fundamental property	43
1.5.2.2. Differentiation property	43
1.5.2.3. Integration property	44
1.5.2.4. Some common transforms	44
1.6. Characteristic function, generating function, z -transform	47
1.6.1. Characteristic function	47
1.6.1.1. Definition	47
1.6.1.2. Inversion formula	48
1.6.1.3. The concept of event indicator and the Heaviside function	48
1.6.1.4. Calculating the inverse function and residues	49
1.6.1.5. The residue theorem	50
1.6.1.6. Asymptotic formula	51
1.6.1.7. Moments	52
1.6.1.8. Some common transforms	53
1.6.2. Generating functions, z -transforms	54
1.6.2.1. Definition	54
1.6.2.2. Moments	54
1.6.2.3. Some common transforms	55
1.6.3. Convolution	56
Chapter 2. Probability Laws	57
2.1. Uniform (discrete) distribution	58
2.2. The binomial law	58

2.3. Multinomial distribution	60
2.4. Geometric distribution	61
2.5. Hypergeometric distribution	62
2.6. The Poisson law	63
2.7. Continuous uniform distribution	65
2.8. Normal (Gaussian) distribution	66
2.9. Chi-2 distribution	70
2.10. Student distribution	71
2.11. Lognormal distribution	72
2.12. Exponential and related distributions	72
2.12.1. Exponential distribution	72
2.12.2. Erlang-k distribution	73
2.12.3. Hyperexponential distribution	75
2.12.4. Generalizing: Coxian distribution	77
2.12.5. Gamma distribution	77
2.12.6. Weibull distribution	78
2.13. Logistic distribution	79
2.14. Pareto distribution	81
2.15. A summary of the main results	82
2.15.1. Discrete distributions	82
2.15.2. Continuous distributions	83
Chapter 3. Statistics	87
3.1. Descriptive statistics	88
3.1.1. Data representation	88
3.1.2. Statistical parameters	90
3.1.2.1. Fractiles	90
3.1.2.2. Sample mean	91
3.1.2.3. Sample variance	91
3.1.2.4. Moments	91
3.1.2.5. Mode	91
3.1.2.6. Other characterizations	92
3.2. Correlation and regression	92
3.2.1. Correlation coefficient	93
3.2.2. The regression curve	94
3.2.2.1. The least squares method	94
3.3. Sampling and estimation techniques	96
3.4. Estimation	97
3.4.1. Point estimation	98
3.4.1.1. Average	99
3.4.1.2. Variance	99
3.4.1.3. Estimating the mean and variance of a normal distribution	100
3.4.1.4. Example: estimating the average lifetime of equipment	101

3.4.2. Estimating confidence intervals	102
3.4.2.1. Example 1: estimating the mean of a normal distribution . . .	104
3.4.2.2. Example 2: Chi-2 distribution in reliability	104
3.4.2.3. Estimating proportion	106
3.4.2.4. Estimating the parameter of a Poisson distribution	108
3.5. Hypothesis testing	108
3.5.1. Example: testing the mean value of a normal distribution	108
3.5.2. Chi-2 test: uniformity of a random generator	110
3.5.3. Correlation test	111
Chapter 4. Signal Theory	113
4.1. Concept of signal and signal processing	113
4.2. Linear time-invariant systems and filtering	115
4.2.1. Linear time-invariant systems	115
4.2.2. Impulse response and convolution function of an LTI system . . .	115
4.2.3. Filtering function	116
4.3. Fourier transform and spectral representation	117
4.3.1. Decomposing a periodic signal using Fourier series	118
4.3.2. Fourier transform of an arbitrary signal	119
4.3.3. Dirac delta function and its Fourier transform	121
4.3.4. Properties of Fourier transforms	124
4.3.4.1. Time and frequency shifts	124
4.3.4.2. Convolution product and filtering	125
4.3.4.3. Product of functions and transform convolution	125
4.3.4.4. Product of functions and modulation	126
4.3.4.5. Energy conservation and Parseval's theorem	129
4.4. Sampling	130
4.4.1. Sampling function	130
4.4.2. Shannon sampling theorem	131
4.5. Quantization and coding	132
4.5.1. Quantization noise	133
4.5.2. Coding power	135
4.6. Discrete LTI system	136
4.7. Transforms for digital signal processing	136
4.7.1. The z -transform	136
4.7.1.1. Definition	137
4.7.1.2. Time translation	137
4.7.1.3. Discrete convolution	138
4.7.1.4. Inversion	139
4.7.2. Fourier transform of a discrete signal	140
4.7.3. Discrete Fourier transform	141
4.7.3.1. Definition	141
4.7.3.2. Properties	143

4.7.4. Cosine transform	144
4.7.5. The fast Fourier transform (FFT)	145
4.7.5.1. Cooley-Tukey FFT algorithm	145
4.8. Filter design and synthesis	146
4.8.1. Definitions and principles	147
4.8.1.1. Principle	147
4.8.1.2. Causality and stability	148
4.8.2. Finite impulse response (FIR) filters	148
4.8.2.1. Design methodology	149
4.8.2.2. FIR filter synthesis	152
4.8.2.3. Low-pass, high-pass and band-pass filters	154
4.8.3. Infinite impulse response (IIR) filters	154
4.8.3.1. Filter design from models of the s plane	156
4.8.3.2. Butterworth model	158
4.8.3.3. Chebychev model	160
4.8.3.4. Synthesis of IIR filters	161
4.8.3.5. Low-pass, high-pass and band-pass filters	162
4.8.4. Non-linear filtering	163
4.8.4.1. Median filtering at rank N	163
4.8.5. Filter banks and multirate systems	164
4.8.5.1. Sub- and up-sampling	165
4.8.5.2. Multirate filtering and polyphase bank	168
4.8.5.3. Signal decomposition and reconstruction	169
4.8.5.4. Half-band filters	171
4.8.5.5. Quadrature mirror filters	172
4.9. Spectral analysis and random signals	173
4.9.1. Statistical characterization of random signals	173
4.9.1.1. Average	174
4.9.1.2. Autocorrelation function	174
4.9.1.3. Power spectral density	176
4.9.2. Filtering a random signal	178
4.9.2.1. Spectral density of a filtered signal	178
4.9.2.2. Filtering white noise	180
4.9.3. Sampled random signals	180
4.9.3.1. Autocorrelation function	181
4.9.3.2. Cross-correlation function	181
4.9.3.3. Power spectral density	181
4.9.4. Filtering a sampled random signal	182
4.9.4.1. Spectral density of the filtered signal	183
4.9.4.2. Correlation between input and output signals (cross-correlation)	183
4.9.4.3. Colored noise	183

- 4.9.5. Spectral estimation 184
 - 4.9.5.1. Estimating the autocorrelation function 184
 - 4.9.5.2. Non-parametric spectral estimation with periodogram 185
 - 4.9.5.3. Parametric spectral estimation: ARMA, AR, MA 187
 - 4.9.5.4. Toeplitz matrix and Levinson algorithm 189
- 4.10. Linear prediction, coding and speech synthesis, adaptive filtering . . . 192
 - 4.10.1. Linear prediction 192
 - 4.10.1.1. Variance minimization 193
 - 4.10.1.2. Example of speech processing: coding and synthesis 194
 - 4.10.2. Adaptive filtering 195
 - 4.10.2.1. The least squares method with exponential forgetting 196
 - 4.10.2.2. The stochastic gradient descent algorithm 197
 - 4.10.2.3. Example: echo cancelation 198

Chapter 5. Information and Coding Theory 201

- 5.1. Information theory 201
 - 5.1.1. The basic diagram of a telecommunication system 202
- 5.2. Information measurement 202
 - 5.2.1. Algebraic definition of information 203
 - 5.2.2. Probabilistic definition of information 203
 - 5.2.3. Self-information 204
 - 5.2.4. Unit of information 204
 - 5.2.5. Conditional information 205
 - 5.2.6. Mutual information 205
- 5.3. Entropy 206
 - 5.3.1. Entropy of a memoryless source 206
 - 5.3.2. Entropy of a binary source 206
 - 5.3.3. Maximum entropy 207
 - 5.3.4. Joint entropy of random variables 208
 - 5.3.5. Average conditional entropy 208
 - 5.3.6. Additivity and joint entropy 209
 - 5.3.7. Average mutual information 210
 - 5.3.8. Conditional average mutual information 210
 - 5.3.9. Extension to the continuous case 210
- 5.4. Source modeling 211
 - 5.4.1. Concept of sources with and without memory 211
 - 5.4.2. Discrete Markov source in discrete time 212
 - 5.4.3. The main types of source 215
 - 5.4.3.1. The binary source 215
 - 5.4.3.2. Text, or alphabetic source 216
 - 5.4.4. Information rate of the source 217
- 5.5. Source coding 217
 - 5.5.1. Code efficiency 217

5.5.2. Redundancy of a code	219
5.5.3. Instantaneous and uniquely decipherable codes	220
5.6. Shannon's first theorem	220
5.6.1. Optimal coding	220
5.6.2. Shannon's first theorem	222
5.7. Coding and data compression	224
5.7.1. Huffman coding algorithm	224
5.7.2. Retrieval algorithms and decision trees	226
5.7.3. (Reversible) data compression	227
5.7.3.1. The Huffman method	228
5.7.3.2. Fano method	229
5.7.3.3. Shannon's method	230
5.7.3.4. Arithmetic coding	230
5.7.3.5. Adaptive and dictionary methods	233
5.7.4. Image compression	234
5.7.4.1. Describing an image: luminance and chrominance	234
5.7.4.2. Image redundancy	236
5.7.4.3. The discrete cosine transform (DCT)	237
5.7.4.4. Quantization and coding	242
5.7.4.5. Recent methods: wavelets	244
5.7.4.6. JPEG2000	250
5.8. Channel modeling	252
5.8.1. Definition of the channel	252
5.8.2. Channel capacity	253
5.8.3. Binary symmetric channel	254
5.9. Shannon's second theorem	254
5.9.1. The noisy-channel coding theorem (Shannon's second theorem)	255
5.10. Error-detecting and error-correcting codes	256
5.10.1. Algebraic coding	257
5.10.1.1. Principles	257
5.10.1.2. Hamming distance	258
5.10.1.3. Detection and correction capability	260
5.10.1.4. Additional definitions and properties	261
5.10.1.5. Linear block codes, group codes	262
5.10.1.6. Cyclic codes	267
5.10.2. Convolutional codes	272
5.10.2.1. D -transform	273
5.10.2.2. Graphical representation, graphs and trellis	273
5.10.2.3. Viterbi's algorithm	275
5.10.3. Combined codes and turbo codes	276
5.10.3.1. Interleaving	277
5.10.3.2. Product codes	278
5.10.3.3. Concatenation	278

5.10.3.4. Parallelization	278
5.10.3.5. Turbo codes	278
5.11. Cryptology	282
5.11.1. Encryption	282
5.11.1.1. Symmetric-key encryption	282
5.11.1.2. Public-key encryption	284
5.11.2. Digital signature	286
5.11.3. Signature and hashing	286
Chapter 6. Traffic and Queueing Theory	289
6.1. Traffic concepts	289
6.1.1. The Erlang concept	290
6.1.2. Traffic modeling	291
6.2. The concept of processes	292
6.2.1. Arrival process	292
6.2.1.1. Renewal process	292
6.2.1.2. Poisson arrivals	293
6.2.1.3. The use of the Poisson process	296
6.2.2. Service process	296
6.2.2.1. Exponential distribution	297
6.2.2.2. Residual service time	297
6.2.2.3. Erlang distribution	299
6.2.2.4. Hyperexponential distribution	299
6.2.3. General arrival and service processes	300
6.3. Markov and birth/death processes	301
6.3.1. State concept	302
6.3.2. Markov chains	302
6.3.3. Birth and death processes	303
6.4. Queueing models	306
6.4.1. Introduction	306
6.4.2. A general result: the Little formula	307
6.4.3. PASTA property (Poisson arrivals see time averages)	309
6.4.4. The elementary queue: the M/M/1 system	310
6.4.4.1. Resolution of the state equations	310
6.4.4.2. Using generating functions	312
6.4.4.3. Waiting time distribution	313
6.4.5. The M/M/R/R model (Erlang model)	317
6.4.6. The M/M/R queue and the Erlang-C formula	318
6.4.7. The M/M/ ∞ queue and the Poisson law	321
6.4.8. The M(n)/M/R/R queue and the Engset formula	322
6.4.9. Models with limited capacity	325
6.5. More complex queues	325
6.5.1. Multi-bitrate Erlang model	325

6.5.2. The embedded Markov chain	326
6.5.3. The number of clients in a system	327
6.5.4. Waiting times: Pollaczek formulae	330
6.5.4.1. Introduction: calculation of residual service time	330
6.5.4.2. The Pollaczek-Khintchine formula	332
6.5.4.3. Example 1: the M/M/1 queue	333
6.5.4.4. Example 2: the M/D/1 queue	333
6.5.4.5. Generalization: Takacs' formula	333
6.5.5. The Beneš method: application to the M/D/1 system	333
6.6. The G/G/1 queue	334
6.6.1. Pollaczek method	335
6.6.2. Application to the stochastic relation of the queue to one server (GI/G/1 queue)	337
6.6.3. Resolution of the integral equation	339
6.6.3.1. Application to the M/G/1 queue	339
6.6.3.2. Application to the G/M/1 queue	343
6.6.4. Other applications and extension of the Pollaczek method	346
6.7. Queues with priorities	347
6.7.1. Work conserving system	348
6.7.2. The HoL discipline	350
6.8. Using approximate methods	351
6.8.1. Reattempts	352
6.8.2. Peakedness factor method	353
6.8.3. Approximate formulae for the G/G/R system	358
6.9. Appendix: Pollaczek transform	359
Chapter 7. Reliability Theory	363
7.1. Definition of reliability	363
7.2. Failure rate and bathtub curve	364
7.3. Reliability functions	365
7.4. System reliability	366
7.4.1. Reliability of non-repairable systems	366
7.4.1.1. Reliability of the series configuration	367
7.4.1.2. Reliability of the parallel configuration	368
7.4.1.3. Reliability of the series-parallel configuration	369
7.4.1.4. Reliability of the parallel-series configuration	370
7.4.1.5. Complex configurations	370
7.4.1.6. Non-repairable redundant configurations	371
7.4.2. Reliability and availability of repairable systems	373
7.4.2.1. State equations	373
7.4.2.2. Reliability of redundant repairable systems	375
7.4.2.3. Imperfect structures	380
7.4.3. Using Laplace transform	382

7.4.4. Use of matrices	385
7.4.4.1. Exact resolution by inversion	387
7.4.4.2. Approximate solutions	389
7.5. Software reliability	390
7.5.1. Reliability growth model, early-life period	391
7.5.2. Useful-life period model	392
7.6. Spare parts calculation	395
7.6.1. Definitions	395
7.6.2. Periodical restocking	396
7.6.3. Continuous restocking	396
Chapter 8. Simulation	399
8.1. Roulette simulation	400
8.2. Discrete-event simulation	402
8.3. Measurements and accuracy	404
8.3.1. Measurements	404
8.3.2. Accuracy	404
8.4. Random numbers	407
8.4.1. Generation according to a distribution	407
8.4.2. Generating pseudo-random variables	408
Appendix. Mathematical Refresher	413
A.1. The function of the complex variable: definition and theorems	413
A.2. Usual z -transforms	415
A.3. Series expansions (real functions)	415
A.4. Series expansion of a function of the complex variable	418
A.5. Algebraic structures	419
A.6. Polynomials over the binary finite field	422
A.7. Matrices	424
Bibliography	427
Index	431

Preface

Communication techniques and services are changing rapidly, and so are the techniques for the design and analysis of communicating systems and networks transporting and processing information: both in terms of data or images generated in a professional environment and – increasingly – in a personal environment (personal terminals: computers and mobiles). We have felt the need to reconsider basic mathematic tools, usually known by engineers but seldom presented as a whole, in the context of communication technologies. So, this book presents the major mathematical techniques in use in the field of telecommunications and more generally in the domain of information and communication technologies. Engineers, as well as students, will be led to tackle problems related to various subjects, such as signal and information processing, traffic or performance analysis, reliability, etc. Possibly they will become specialists, or responsible for one or several of these domains. We attempt here to provide the mathematical basis necessary to open constructive exchanges with experts, and also to efficiently begin the study of specialized publications.

The present publication has naturally been constructed around the notion of probability. Indeed, we should not be surprised that random variables play a major role in the mathematics deployed to solve problems related to the processing and transport of “information”, in essence an unknown quantity. This has naturally guided the structure of this book, providing something of a framework for a unified theoretical approach of communications, with the following chapters.

Probability theory is naturally the subject of Chapter 1, as it constitutes the basis of numerous developments in all the fields addressed by this book, from simple combinatorics to queueing theory, signal processing, statistics or reliability. The chapter presents the main theorems and introduces the notion of random variables and their handling. Transform properties, and their use, are also detailed. Indeed, transforms happen to offer an essential tool for the solution of numerous problems

arising when dealing with linear systems, birth and death systems or stochastic relationships. They will find many applications in each of the following chapters.

Chapter 2 complements Chapter 1 and presents the major *probability distributions* we should encounter when describing or modeling the events observed in systems and networks. This refers to, for instance, the analysis of a signal, the volume of data to process, or the reliability of a piece of equipment. All these distributions will be of constant use in the later chapters.

Statistics constitute the object of Chapter 3. Engineers face uncertainty at every step – in observation, measurement, modeling – and have to rely on statistical techniques in order to support their decisions. Estimation will be a constant necessity, e.g. when observing traffic flows, measuring equipment reliability or recognizing a signal.

Chapter 4 presents *signal theory* and its *digital processing*. Every communication relies on signals, and more and more sophisticated methods guarantee the quality of its transport and reconstruction. Sampling makes it possible to represent the actual analog signal in the form of a digital signal. The latter can then be easily stored or transported. Finally, digital processing techniques allow signal filtering in order to restore it as accurately as possible, or even to synthesize new signals. The complex variable, the Fourier and z -transforms, as well as correlation analysis are the major tools for these operations.

Chapter 5, devoted to *information and coding theory*, is the natural successor of Chapter 4. Considering the random nature of information and its perturbations, digitalization and coding bring considerable improvements, both for its transmission (error correction) and for resource optimization (thanks to compression techniques). The chapter first presents a probabilistic model of the information (measure of information and notion of entropy, source and channel modeling, Shannon's theorems), then the major theoretical and practical aspects of coding algorithms are introduced (detecting codes and correcting codes, data compression, for text, image and sounds). For this, probabilities, transforms and modulo 2 algebra will be used.

Chapter 6 presents *traffic and queueing theory*. In networks, traffic represents the information transported globally, its volume, time characteristics (arrival epochs, duration of resource seizing). Here we encounter the well-known *Erlang* concept and the associated dimensioning procedures. Traffic and queueing theory are the essential tools for performance analysis of networks and computers, in order to guarantee the fulfilment of quality of service constraints, through systems and protocols modeling. This is above all the area of Markov processes, of stochastic relations as well as Laplace transforms, generating and characteristic functions.

Chapter 7 presents *reliability theory*. Facing all defects present in any equipment and software involved in a given communication task, and given the catalectic