ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

FOUNDING EDITOR G.-C. ROTA

Volume 86

The Theory of Information and Coding
Second Edition

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

4 W. Miller, Jr. *Symmetry and separation of variables*
6 H. Minc *Permanents*
11 W. B. Jones and W. J. Thron *Continued fractions*
12 N. F. G. Martin and J. W. England *Mathematical theory of entropy*
18 H. O. Fattorini *The Cauchy problem*
19 G. G. Lorentz, K. Jetter and S. D. Riemenschneider *Birkhoff interpolation*
21 W. T. Tutte *Graph theory*
22 J. R. Bastida *Field extensions and Galois theory*
23 J. R. Cannon *The one-dimensional heat equation*
25 A. Salomaa *Computation and automata*
26 N. White (ed.) *Theory of matroids*
27 N. H. Bingham, C. M. Goldie and J. L. Teugels *Regular variation*
28 P. P. Petrushev and V. A. Popov *Rational approximation of real functions*
29 N. White (ed.) *Combinatorial geometrics*
30 M. Pohst and H. Zassenhaus *Algorithmic algebraic number theory*
31 J. Aczel and J. Dhombres *Functional equations containing several variables*
32 M. Kuczma, B. Chozewski and R. Ger *Iterative functional equations*
33 R. V. Ambartzumian *Factorization calculus and geometric probability*
34 G. Gripenberg, S.-O. Londen and O. Staffans *Volterra integral and functional equations*
35 G. Gasper and M. Rahman *Basic hypergeometric series*
36 E. Torgersen *Comparison of statistical experiments*
37 A. Neumaier *Intervals methods for systems of equations*
38 N. Korneichuk *Exact constants in approximation theory*
39 R. A. Brualdi and H. J. Ryser *Combinatorial matrix theory*
40 N. White (ed.) *Matroid applications*
41 S. Sakai *Operator algebras in dynamical systems*
42 W. Hodges *Model theory*
43 H. Stahl and V. Totik *General orthogonal polynomials*
44 R. Schneider *Convex bodies*
45 G. Da Prato and J. Zabczyk *Stochastic equations in infinite dimensions*
46 A. Bjorner, M. Las Vergnas, B. Sturmfels, N. White and G. Ziegler *Oriented matroids*
47 E. A. Edgar and L. Sucheston *Stopping times and directed processes*
48 C. Sims *Computation with finitely presented groups*
49 T. Palmer *Banach algebras and the general theory of* **-algebras*
50 F. Borceux *Handbook of categorical algebra I*
51 F. Borceux *Handbook of categorical algebra II*
52 F. Borceux *Handbook of categorical algebra III*
54 A. Katok and B. Hassleblatt *Introduction to the modern theory of dynamical systems*
55 V. N. Sachkov *Combinatorial methods in discrete mathematics*
56 V. N. Sachkov *Probabilistic methods in discrete mathematics*
57 P. M. Cohn *Skew Fields*
58 Richard J. Gardner *Geometric tomography*
59 George A. Baker, Jr. and Peter Graves-Morris *Padé approximants*
60 Jan Krajicek *Bounded arithmetic, propositional logic, and complex theory*
61 H. Gromer *Geometric applications of Fourier series and spherical harmonics*
62 H. O. Fattorini *Infinite dimensional optimization and control theory*
63 A. C. Thompson *Minkowski geometry*
64 R. B. Bapat and T. E. S. Raghavan *Nonnegative matrices and applications*
65 K. Engel *Sperner theory*
66 D. Cvetkovic, P. Rowlinson and S. Simic *Eigenspaces of graphs*
67 F. Bergeron, G. Labelle and P. Leroux *Combinatorial species and tree-like structures*
68 R. Goodman and N. Wallach *Representations of the classical groups*
69 T. Beth, D. Jungnickel and H. Lenz *Design Theory volume I 2 ed.*
70 A. Pietsch and J. Wenzel *Orthonormal systems and Banach space geometry*
71 George E. Andrews, Richard Askey and Ranjan Roy *Special Functions*
72 R. Ticciati *Quantum field theory for mathematicians*
76 A. A. Ivanov *Geometry of sporadic groups I*
78 T. Beth, D. Jungnickel and H. Lenz *Design Theory volume II 2 ed.*
80 O. Stormark *Lie's Structural Approach to PDE Systems*
81 C. F. Dunkl and Y. Xu *Orthogonal polynomials of several variables*
82 J. Mayberry *The foundations of mathematics in the theory of sets*
83 C. Foias, R. Temam, O. Manley and R. Martins da Silva Rosa *Navier–Stokes equations and turbulence*
84 B. Polster and G. Steinke *Geometries on Surfaces*
85 D. Kaminski and R. B. Paris *Asymptotics and Mellin–Barnes integrals*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

The Theory of Information and Coding
Second Edition

R. J. McELIECE
California Institute of Technology

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India

103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521000956

Published by Addison-Wesley 1977, 1979, 1982

First published by Cambridge University Press 1985

Second edition 2002
Reprinted 2003

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-00095-6 Hardback

Contents

Editor's statement

A large body of mathematics consists of facts that can be presented and described much like any other natural phenomenon. These facts, at times explicitly brought out as theorems, at other times concealed within a proof, make up most of the applications of mathematics, and are the most likely to survive changes of style and of interest.

This ENCYCLOPEDIA will attempt to present the factual body of all mathematics. Clarity of exposition, accessibility to the non-specialist, and a thorough bibliography are required of each author. Volumes will appear in no particular order, but will be organized into sections, each one comprising a recognizable branch of present-day mathematics. Numbers of volumes and sections will be reconsidered as times and needs change.

It is hoped that this enterprise will make mathematics more widely used where it is needed, and more accessible in fields in which it can be applied but where it has not yet penetrated because of insufficient information.

Information theory is a success story in contemporary mathematics. Born out of very real engineering problems, it has left its imprint on such far-flung endeavors as the approximation of functions and the central limit theorem of probability. It is an idea whose time has come.

Most mathematicians cannot afford to ignore the basic results in this field. Yet, because of the enormous outpouring of research, it is difficult for anyone who is not a specialist to single out the basic results and the relevant material. Robert McEliece has succeeded in giving a presentation that achieves this objective, perhaps the first of its kind.

GIAN-CARLO ROTA

Foreword

Transmission of information is at the heart of what we call communication. As an area of concern it is so vast as to touch upon the preoccupations of philosophers and to give rise to a thriving technology.

We owe to the genius of Claude Shannon* the recognition that a large class of problems related to encoding, transmitting, and decoding information can be approached in a systematic and disciplined way: his classic paper of 1948 marks the birth of a new chapter of Mathematics.

In the past thirty years there has grown a staggering literature in this fledgling field, and some of its terminology even has become part of our daily language.

The present monograph (actually two monographs in one) is an excellent introduction to the two aspects of communication: coding and transmission.

The first (which is the subject of Part two) is an elegant illustration of the power and beauty of Algebra; the second belongs to Probability Theory which the chapter begun by Shannon enriched in novel and unexpected ways.

MARK KAC
General Editor, Section on Probability

* C. E. Shannon, A Mathematical Theory of Communication, *Bell System Tech. J.* **27** (1948), Introduction: 379–382; Part one: Discrete Noiseless Systems, 382–405; Part two: The Discrete Channel with Noise (and Appendixes), 406–423; Part III: Mathematical Preliminaries, 623–636; Part IV: The Continuous Channel (and Appendixes), 637–656).

Preface to the first edition

This book is meant to be a self-contained introduction to the basic results in the theory of information and coding. It was written during 1972–1976, when I taught this subject at Caltech. About half my students were electrical engineering graduate students; the others were majoring in all sorts of other fields (mathematics, physics, biology, even one English major!). As a result the course was aimed at nonspecialists as well as specialists, and so is this book.

The book is in three parts: Introduction, Part one (Information Theory), and Part two (Coding Theory). It is essential to read the introduction first, because it gives an overview of the whole subject. In Part one, Chapter 1 is fundamental, but it is probably a mistake to read it first, since it is really just a collection of technical results about entropy, mutual information, and so forth. It is better regarded as a reference section, and should be consulted as necessary to understand Chapters 2–5. Chapter 6 is a survey of advanced results, and can be read independently. In Part two, Chapter 7 is basic and must be read before Chapters 8 and 9; but Chapter 10 is almost, and Chapter 11 is completely, independent from Chapter 7. Chapter 12 is another survey chapter independent of everything else.

The problems at the end of the chapters are very important. They contain verification of many omitted details, as well as many important results not mentioned in the text. It is a good idea to at least read the problems.

There are four appendices. Appendix A gives a brief survey of probability theory, essential for Part one. Appendix B discusses convex functions and Jensen's inequality. Appendix C sketches the main results about finite fields needed in Chapter 9. Appendix D describes an algorithm for counting paths in directed graphs which is needed in Chapter 10.

A word about cross-references is in order: sections, figures, examples, theorems, equations, and problems are numbered consecutively by chapters, using double numeration. Thus "Section 2.3," "Theorem 3.4," and "Prob. 4.17" refer to section 3 of Chapter 2, Theorem 4 of Chapter 3, and Problem 17 of Chapter 4, respectively. The appendices are referred to by letter; thus "Equation (B.4)" refers to the fourth numbered equation in Appendix B.

The following special symbols perhaps need explanation: "□" signals the end of a proof or example; "iff" means *if and only if*; $\lfloor x \rfloor$ denotes the largest integer $\leqslant x$; and $\lceil x \rceil$ denotes the smallest integer $\geqslant x$.

Finally, I am happy to acknowledge my debts: To Gus Solomon, for introducing me to the subject in the first place; to John Pierce, for giving me the opportunity to teach at Caltech; to Gian-Carlo Rota, for encouraging me to write this book; to Len Baumert, Stan Butman, Gene Rodemich, and Howard Rumsey, for letting me pick their brains; to Jim Lesh and Jerry Heller, for supplying data for Figures 6.7 and 12.2; to Bob Hall, for drafting the figures; to my typists, Ruth Stratton, Lillian Johnson, and especially Dian Rapchak; and to Ruth Flohn for copy editing.

ROBERT J. MCELIECE

Preface to the second edition

The main changes in this edition are in Part two. The old Chapter 8 ("BCH, Goppa, and Related Codes") has been revised and expanded into two new chapters, numbered 8 and 9. The old chapters 9, 10, and 11 have then been renumbered 10, 11, and 12. The new Chapter 8 ("Cyclic codes") presents a fairly complete treatment of the mathematical theory of cyclic codes, and their implementation with shift register circuits. It culminates with a discussion of the use of cyclic codes in burst error correction. The new Chapter 9 ("BCH, Reed–Solomon, and Related Codes") is much like the old Chapter 8, except that increased emphasis has been placed on Reed-Solomon codes, reflecting their importance in practice. Both of the new chapters feature dozens of new problems.