Fundamentals of Classical and Modern Error-Correcting Codes

Using easy-to-follow mathematics, this textbook provides comprehensive coverage of block codes and techniques for reliable communications and data storage. It covers major code designs and constructions from geometric, algebraic, and graph-theoretic points of view, decoding algorithms, error-control additive white Gaussian noise (AWGN) and erasure, and reliable data recovery. It simplifies a highly mathematical subject to a level that can be understood and applied with a minimum background in mathematics, provides step-by-step explanation of all covered topics, both fundamental and advanced, and includes plenty of practical illustrative examples to assist understanding. Numerous homework problems are included to strengthen student comprehension of new and abstract concepts, and a solution manual is available online for instructors. Modern developments, including polar codes, are also covered.

This is an essential textbook for senior undergraduates and graduates taking introductory coding courses, students taking advanced full-year graduate coding courses, and professionals working on coding for communications and data storage.

Shu Lin is Adjunct Professor in the Department of Electrical and Computer Engineering at the University of California, Davis, and an IEEE Life Fellow. He has authored and coauthored several books, including *LDPC Code Designs, Constructions, and Unification* (Cambridge University Press, 2016) and *Channel Codes: Classical and Modern* (Cambridge University Press, 2009).

Juane Li is Staff Systems Architect at Micron Technology Inc., San Jose, having previously completed her PhD at the University of California, Davis. She is also a coauthor of *LDPC Code Designs, Constructions, and Unification* (Cambridge University Press, 2016).

Fundamentals of Classical and Modern Error-Correcting Codes

SHU LIN
University of California, Davis

JUANE LI
Micron Technology Inc., San Jose

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/highereducation/isbn/9781316512623
DOI: 10.1017/9781009067928

First published 2022

Printed in the United Kingdom by TJ Books Limited, Padstow, Cornwall, 2022

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

Library of Congress Cataloging-in-Publication Data
Names: Lin, Shu, 1937– author. | Li, Juane, author.
Title: Fundamentals of classical and modern error-correcting codes / Shu Lin, University of California, Davis, Juane Li, Micron Technology, San Jose.
Description: Cambridge, United Kingdom ; New York, NY, USA : Cambridge University Press, 2021. | Includes bibliographical references and index.
Identifiers: LCCN 2021025406 (print) | LCCN 2021025407 (ebook) | ISBN 9781316512623 (hardback) | ISBN 9781009067928 (epub)
Subjects: LCSH: Error-correcting codes (Information theory)
Classification: LCC TK5102.96 .L53 2021 (print) | LCC TK5102.96 (ebook) | DDC 005.7/2–dc23
LC record available at https://lccn.loc.gov/2021025406
LC ebook record available at https://lccn.loc.gov/2021025407

ISBN 978-1-316-51262-3 Hardback

Additional resources for this publication at www.cambridge.org/lin-li

Cambridge University Press
978-1-316-51262-3 — Fundamentals of Classical and Modern Error-Correcting Codes
Shu Lin , Juane Li
Frontmatter
More Information

Contents

Cambridge University Press
978-1-316-51262-3 — Fundamentals of Classical and Modern Error-Correcting Codes
Shu Lin , Juane Li
Frontmatter
More Information

Figures

Cambridge University Press
978-1-316-51262-3 — Fundamentals of Classical and Modern Error-Correcting Codes
Shu Lin , Juane Li
Frontmatter
More Information

Tables

Preface

One of the serious problems in a digital data communication or storage system is the occurrence of errors caused by noise and interference in communication channels or imperfections in storage mediums. A major concern to the communication or storage-system designers is the control of these errors such that reliable transmission or storage of data can be achieved. In 1948, Shannon demonstrated in a landmark paper that by proper encoding and decoding of the data, errors induced by a noisy channel or imperfect storage medium can be reduced to any desired level without sacrificing the rate of information transmission or storage, as long as the information rate is less than the capacity of the channel or the storage medium. Since Shannon's work, a tremendous amount of research effort has been expended on the problems of devising efficient encoding and decoding methods and techniques for error control on noisy channels or imperfect storage mediums. As a result of this research effort, various efficient encoding and decoding methods and techniques have been developed to achieve the reliability required by today's explosive high-speed and large-volume digital communication and storage systems.

Much of the work on error-correcting codes (or error-control codes) developed since 1948 is highly mathematical in nature, and a thorough understanding requires an extensive background in modern algebra, combinatorial mathematics, and graph theory. This requirement may impede senior and first-year graduate students in electrical and computer engineering who are interested in learning and pursuing research in coding theory, and practicing engineers in industry who are interested in applying error-control coding techniques to practical systems.

One of the objectives of this book is to bring this highly complex material down to a reasonably simple level such that it can be understood and applied with a minimum background in mathematics. To achieve this objective, we take a middle ground between mathematical rigor and heuristic reasoning as the first author did in his first book on the introduction to error-correcting codes published in 1970. Because of the extensive developments in error-correcting codes over the past 50 years, it is not possible to include certain categories of error-correcting codes in this book. The main coverage of this book is the fundamental and essential aspects of codes with block structure, called block codes, and their up-to-date developments in construction, encoding, and decoding techniques. The presentation of these subjects is intended to be comprehensive. In presenting every step of each topic in the book, illustrative examples are given to assist the readers to follow and fully understand the topic with a minimum barrier. Furthermore, derivations and long proofs that are not helpful in illustration of a topic are avoided. Long essential derivations or proofs of any topic are put in the appendices or referred to in published article(s).

In the following, a brief description of major coverage in each chapter is presented. Chapter 1 gives a brief overview of coding for error control in information transmission and data storage. Chapter 2 provides the readers with an elementary knowledge of modern algebra and graph theory that will aid in understanding the fundamental and essential aspects of error-correcting codes to be developed in the other chapters of the book. Chapter 3 gives an introduction to block codes with linear structure, called linear block codes, their structural properties, and general decoding methods. Chapter 4 introduces two special categories of linear block codes with cyclic and quasi-cyclic structures, called cyclic codes and quasi-cyclic codes, respectively. Also presented in this chapter are two small classes of cyclic codes, known as Hamming and quadratic-residue (QR) codes.

Chapters 5 and 6 present two well-known classes of cyclic codes constructed based on finite fields, called the Bose–Chaudhuri–Hocquenghem (BCH) and the Reed–Solomon (RS) codes. These two classes of cyclic codes have been widely used in digital-communication and data-storage systems. Major topics covered in these two chapters include code constructions, characterizations, and decoding algorithms. Presented in Chapter 7 are two classes of cyclic codes constructed based on two categories of finite geometries, named Euclidean and projective geometries. Finite-geometry codes in these two classes are low-density parity-check (LDPC) codes, which can be decoded with iterative soft-decision algorithms based on belief-propagation to achieve good error performance with practical implementation complexity.

Chapter 8 presents another well-known class of linear block codes, called Reed–Muller (RM) codes, for correcting multiple random errors. RM codes can be decoded with a simple majority-logic decoding algorithm using a successive-cancellation process. Chapter 9 presents several coding techniques that are commonly used in communication and storage systems for reliable information transmission and data storage. These coding techniques include: (1) interleaving; (2) direct product; (3) concatenation; (4) turbo coding; (5) $|\mathbf{u}|\mathbf{u}+\mathbf{v}|$-construction; (6) Kronecker (or tensor) product; and (7) automatic-request-retransmission (ARQ) schemes. Chapter 10 presents various types of codes and coding techniques for correcting bursts of errors, random erasures, bursts of erasures, and combinations of random errors and erasures. Also presented in this chapter is a simple successive-peeling algorithm for correcting random erasures.

Chapter 11 introduces LDPC codes which can achieve near-capacity (or close to Shannon-limit) performance with iterative soft-decision decoding based on belief-propagation over various communication and data-storage channels. Many LDPC codes have been adopted as standard codes for various current and next-generation communication systems. Major aspects covered in this chapter include: (1) basic concepts and characteristics; (2) matrix and graphical representations; (3) various iterative decoding algorithms based on belief-propagation; and (4) error performances over binary-input additive white Gaussian noise (AWGN) and erasure channels.

Chapters 12–14 present three classes of cyclic and quasi-cyclic LDPC codes that are constructed based on finite and partial geometries, finite fields, and experimental designs. These LDPC codes achieve good error performance on both binary-input AWGN and binary-erasure channels. Also included in these chapters are two reduced-complexity iterative decoding algorithms and a technique, called masking, for performance enhancement of LDPC codes. Chapter 15 presents two graphical methods for constructing LDPC codes, known as protograph and progressive-edge-growth methods. LDPC codes constructed based on protographs form a class of channel capacity approaching codes.

Chapter 16 presents a universal coding scheme for collective encoding and collective iterative soft-decision decoding of cyclic codes of prime lengths in the frequency domain. Collective encoding and decoding allows for reliability in information sharing among the received codewords during the decoding process. This collective decoding and information sharing can achieve a decoding gain over the maximum-likelihood decoding of individually received codewords. Collective encoding and decoding of BCH, RS, and QR codes are covered in this chapter.

Chapter 17 presents a class of channel-capacity-approaching codes, called polar codes. Essential aspects covered in this chapter include: (1) Kronecker matrices, mappings, and vector spaces; (2) polar codes from Kronecker mapping point of view; (3) multilevel encoding of polar codes; (4) construction of polar codes based on channel polarization; and (5) successive-cancellation decoding of polar codes.

Except for the first chapter, all other chapters contain a good number of problems. The problems are of various types, including those that require routine calculations, those that require computer solution or simulation, those that require derivations and proofs, and those that require designs and performance analysis. The problems are selected to strengthen students' or engineers' knowledge of the materials in each chapter.

This book can be used as a text for an introductory course on coding at the senior or beginning-graduate level or a more-comprehensive full-year graduate course. It can also be used as a self-guide for practicing engineers and computer scientists in industry who desire to learn the fundamentals and essentials of coding aspects and how they can be applied to the design of error-control systems. For a one-semester introductory course, the fundamentals presented in Chapters 1–6 and some selected topics in Chapters 7–11 can be used. For a two-semester sequence in coding theory, the first 10 chapters in fundamentals of coding can be used for the first semester and remaining chapters on advanced coding topics in the second semester. The book can also be used as a text for one-semester advanced-graduate course focused on LDPC and polar codes and collective encoding and decoding of cyclic codes of prime lengths. In this case, the instructor could use Chapters 11–17 or selected topics from Chapters 4–8. Furthermore, the materials covered in Chapters 1–4 can be used as supplementary subjects for an undergraduate course in information theory or digital-communication systems.

Acknowledgments

The first author (Shu Lin) would like to take this opportunity to acknowledge the late Professor Paul E. Pfeiffer, the late Professor Wesley W. Peterson, the late Professor Tadao Kasami, and Professor Franklin F. Kuo, who motivated, inspired, and guided him into the wonderful, elegant, and practically useful domain of coding theory at the beginning of his research career. Professor Pfeiffer was his thesis advisor at Rice University. Professor Peterson and Professor Kasami were two pioneers in coding theory, and Professor Peterson wrote the first and most influential book on error-correcting codes. Professor Kou is one of the founders of the Aloha system. Next, the first author would like to thank Professor Ian F. Blake, Professor Dan J. Costello, Jr., Professor Khaled A. S. Abdel-Ghaffar, and Professor William E. Ryan who closely worked with him over many years and helped him to broaden his knowledge in coding theory and its applications in digital communication and data-storage systems. Professor Costello is also his coauthor of two other books.

The most important person behind the first author during the past 57 years, which include the final two years of his graduate study and his entire teaching and research career, is his wife, Ivy. Without her love, support, tolerance, and comfort, as well as raising their three children, his teaching and research career would not have reached as many students or lasted as long as it has. She even took a course in modern algebra to understand what the author was working on at the beginning of his teaching career and to improve their communication. Any success the first author has, he owes to her. She is the one who encouraged him to write this book with his coauthor. So, it is here the first author says to his wife, I love you. Also, the first author would like to give his love and special thanks to his children, their spouses, and grandchildren for their continuing love and affection through the years.

The second author (Juane Li) expresses her sincere gratitude to her advisors, Professor Shu Lin and Professor Khaled A. S. Abdel-Ghaffar, for their valuable guidance, support, and encouragement during her graduate study at the University of California at Davis and during days after her graduation. Professor Lin has rich knowledge, profound ideas, and endless enthusiasm in the error-correcting coding research area. Professor Abdel-Ghaffar is knowledgeable, mathematically rigorous, precise, and patient with students. These two professors' critical and constructive suggestions have pushed her work to a higher level. She also owes a special debt of gratitude to her family for their affection, encouragement, and support over the years.

Both authors are very grateful to Professor Ian F. Blake, Professor Harry Tan, Professor Shih-Chun Chang, Professor William E. Ryan, and Professor Khaled A. S. Abdel-Ghaffar who expended tremendous effort in reading through this book in detail and provided critical comments and numerous valuable suggestions. They would also like to express their appreciation to Professor Qin Huang and Professor Mona Nasseri, Dr. Keke Liu, and Dr. Xin Xiao for their contributions to several topics in this book. They also acknowledge the talented Dr. Zijian Wu who provided such a beautiful photograph of a lotus for the cover image of their book. Last but not least, the authors would like to thank Dr. Julie Lancashire at Cambridge University Press. Without her strong encouragement, warm support, and patience, we would not have been able to bring this book to fruition. Julie, you are a top and thoughtful editor and a good friend.

Cambridge University Press
978-1-316-51262-3 — Fundamentals of Classical and Modern Error-Correcting Codes
Shu Lin , Juane Li
Frontmatter
More Information