Fundamentals of Error-Correcting Codes

Fundamentals of Error-Correcting Codes is an in-depth introduction to coding theory from both an engineering and mathematical viewpoint. As well as covering classical topics, much coverage is included of recent techniques that until now could only be found in specialist journals and book publications. Numerous exercises and examples and an accessible writing style make this a lucid and effective introduction to coding theory for advanced undergraduate and graduate students, researchers and engineers, whether approaching the subject from a mathematical, engineering, or computer science background.

Professor W. Cary Huffman graduated with a PhD in mathematics from the California Institute of Technology in 1974. He taught at Dartmouth College and Union College until he joined the Department of Mathematics and Statistics at Loyola in 1978, serving as chair of the department from 1986 through 1992. He is an author of approximately 40 research papers in finite group theory, combinatorics, and coding theory, which have appeared in journals such as the *Journal of Algebra*, *IEEE Transactions on Information Theory*, and the *Journal of Combinatorial Theory*.

Professor Vera Pless was an undergraduate at the University of Chicago and received her PhD from Northwestern in 1957. After ten years at the Air Force Cambridge Research Laboratory, she spent a few years at MIT's project MAC. She joined the University of Illinois-Chicago's Department of Mathematics, Statistics, and Computer Science as a full professor in 1975 and has been there ever since. She is a University of Illinois Scholar and has published over 100 papers.

Fundamentals of Error-Correcting Codes

W. Cary Huffman
Loyola University of Chicago

and

Vera Pless
University of Illinois at Chicago

CAMBRIDGE UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521131704

First published 2003
This digitally printed version 2010

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

Library of Congress Cataloguing in Publication data

Huffman, W. C. (William Cary)
Fundamentals of error-correcting codes / W. Cary Huffman, Vera Pless.
p. cm.
Includes bibliographical references and index.
ISBN 0 521 78280 5
1. Error-correcting codes (Information theory) I. Pless, Vera. II. Title.
QA268 .H84 2003
005.7′2 – dc21 2002067236

ISBN 978-0-521-78280-7 Hardback
ISBN 978-0-521-13170-4 Paperback

To Gayle, Kara, and Jonathan
Bill, Virginia, and Mike
Min and Mary
Thanks for all your strength and encouragement
W. C. H.

To my children Nomi, Ben, and Dan
for their support
and grandchildren Lilah, Evie, and Becky
for their love
V. P.

Contents

Preface

Coding theory originated with the 1948 publication of the paper "A mathematical theory of communication" by Claude Shannon. For the past half century, coding theory has grown into a discipline intersecting mathematics and engineering with applications to almost every area of communication such as satellite and cellular telephone transmission, compact disc recording, and data storage.

During the 50th anniversary year of Shannon's seminal paper, the two volume *Handbook of Coding Theory*, edited by the authors of the current text, was published by Elsevier Science. That Handbook, with contributions from 33 authors, covers a wide range of topics at the frontiers of research. As editors of the Handbook, we felt it would be appropriate to produce a textbook that could serve in part as a bridge to the Handbook. This textbook is intended to be an in-depth introduction to coding theory from both a mathematical and engineering viewpoint suitable either for the classroom or for individual study. Several of the topics are classical, while others cover current subjects that appear only in specialized books and journal publications. We hope that the presentation in this book, with its numerous examples and exercises, will serve as a lucid introduction that will enable readers to pursue some of the many themes of coding theory.

Fundamentals of Error-Correcting Codes is a largely self-contained textbook suitable for advanced undergraduate students and graduate students at any level. A prerequisite for this book is a course in linear algebra. A course in abstract algebra is recommended, but not essential. This textbook could be used for at least three semesters. A wide variety of examples illustrate both theory and computation. Over 850 exercises are interspersed at points in the text where they are most appropriate to attempt. Most of the theory is accompanied by detailed proofs, with some proofs left to the exercises. Because of the number of examples and exercises that directly illustrate the theory, the instructor can easily choose either to emphasize or deemphasize proofs.

In this preface we briefly describe the contents of the 15 chapters and give a suggested outline for the first semester. We also propose blocks of material that can be combined in a variety of ways to make up subsequent courses. Chapter 1 is basic with the introduction of linear codes, generator and parity check matrices, dual codes, weight and distance, encoding and decoding, and the Sphere Packing Bound. The Hamming codes, Golay codes, binary Reed–Muller codes, and the hexacode are introduced. Shannon's Theorem for the binary symmetric channel is discussed. Chapter 1 is certainly essential for the understanding of the remainder of the book.

Chapter 2 covers the main upper and lower bounds on the size of linear and nonlinear codes. These include the Plotkin, Johnson, Singleton, Elias, Linear Programming, Griesmer,

Gilbert, and Varshamov Bounds. Asymptotic versions of most of these are included. MDS codes and lexicodes are introduced.

Chapter 3 is an introduction to constructions and properties of finite fields, with a few proofs omitted. A quick treatment of this chapter is possible if the students are familiar with constructing finite fields, irreducible polynomials, factoring polynomials over finite fields, and Galois theory of finite fields. Much of Chapter 3 is immediately used in the study of cyclic codes in Chapter 4. Even with a background in finite fields, cyclotomic cosets (Section 3.7) may be new to the student.

Chapter 4 gives the basic theory of cyclic codes. Our presentation interrelates the concepts of idempotent generator, generator polynomial, zeros of a code, and defining sets. Multipliers are used to explore equivalence of cyclic codes. Meggitt decoding of cyclic codes is presented as are extended cyclic and affine-invariant codes.

Chapter 5 looks at the special families of BCH and Reed–Solomon cyclic codes as well as generalized Reed–Solomon codes. Four decoding algorithms for these codes are presented. Burst errors and the technique of concatenation for handling burst errors are introduced with an application of these ideas to the use of Reed–Solomon codes in the encoding and decoding of compact disc recorders.

Continuing with the theory of cyclic codes, Chapter 6 presents the theory of duadic codes, which include the family of quadratic residue codes. Because the complete theory of quadratic residue codes is only slightly simpler than the theory of duadic codes, the authors have chosen to present the more general codes and then apply the theory of these codes to quadratic residue codes. Idempotents of binary and ternary quadratic residue codes are explicitly computed. As a prelude to Chapter 8, projective planes are introduced as examples of combinatorial designs held by codewords of a fixed weight in a code.

Chapter 7 expands on the concept of weight distribution defined in Chapter 1. Six equivalent forms of the MacWilliams equations, including the Pless power moments, that relate the weight distributions of a code and its dual, are formulated. MDS codes, introduced in Chapter 2, and coset weight distributions, introduced in Chapter 1, are revisited in more depth. A proof of a theorem of MacWilliams on weight preserving transformations is given in Section 7.9.

Chapter 8 delineates the basic theory of block designs particularly as they arise from the supports of codewords of fixed weight in certain codes. The important theorem of Assmus–Mattson is proved. The theory of projective planes in connection with codes, first introduced in Chapter 6, is examined in depth, including a discussion of the nonexistence of the projective plane of order 10.

Chapter 9 consolidates much of the extensive literature on self-dual codes. The Gleason–Pierce–Ward Theorem is proved showing why binary, ternary, and quaternary self-dual codes are the most interesting self-dual codes to study. Gleason polynomials are introduced and applied to the determination of bounds on the minimum weight of self-dual codes. Techniques for classifying self-dual codes are presented. Formally self-dual codes and additive codes over $\mathbb{F}_4$, used in correcting errors in quantum computers, share many properties of self-dual codes; they are introduced in this chapter.

The Golay codes and the hexacode are the subject of Chapter 10. Existence and uniqueness of these codes are proved. The Pless symmetry codes, which generalize the ternary Golay

codes, are defined and some of their properties are given. The connection between codes and lattices is developed in the final section of the chapter.

The theory of the covering radius of a code, first introduced in Chapter 1, is the topic of Chapter 11. The covering radii of BCH codes, Reed–Muller codes, self-dual codes, and subcodes are examined. The length function, a basic tool in finding bounds on the covering radius, is presented along with many of its properties.

Chapter 12 examines linear codes over the ring $\mathbb{Z}_4$ of integers modulo 4. The theory of these codes is compared and contrasted with the theory of linear codes over fields. Cyclic, quadratic residue, and self-dual linear codes over $\mathbb{Z}_4$ are defined and analyzed. The nonlinear binary Kerdock and Preparata codes are presented as the Gray image of certain linear codes over $\mathbb{Z}_4$, an amazing connection that explains many of the remarkable properties of these nonlinear codes. To study these codes, Galois rings are defined, analogously to extension fields of the binary field.

Chapter 13 presents a brief introduction to algebraic geometry which is sufficient for a basic understanding of algebraic geometry codes. Goppa codes, generalized Reed–Solomon codes, and generalized Reed–Muller codes can be realized as algebraic geometry codes. A family of algebraic geometry codes has been shown to exceed the Gilbert–Varshamov Bound, a result that many believed was not possible.

Until Chapter 14, the codes considered were block codes where encoding depended only upon the current message. In Chapter 14 we look at binary convolutional codes where each codeword depends not only on the current message but on some messages in the past as well. These codes are studied as linear codes over the infinite field of binary rational functions. State and trellis diagrams are developed for the Viterbi Algorithm, one of the main decoding algorithms for convolutional codes. Their generator matrices and free distance are examined.

Chapter 15 concludes the textbook with a look at soft decision and iterative decoding. Until this point, we had only examined hard decision decoding. We begin with a more detailed look at communication channels, particularly those subject to additive white Gaussian noise. A soft decision Viterbi decoding algorithm is developed for convolutional codes. Low density parity check codes and turbo codes are defined and a number of decoders for these codes are examined. The text concludes with a brief history of the application of codes to deep space exploration.

The following chapters and sections of this book are recommended as an introductory one-semester course in coding theory:

- Chapter 1 (except Section 1.7),
- Sections 2.1, 2.3.4, 2.4, 2.7–2.9,
- Chapter 3 (except Section 3.8),
- Chapter 4 (except Sections 4.6 and 4.7),
- Chapter 5 (except Sections 5.4.3, 5.4.4, 5.5, and 5.6), and
- Sections 7.1–7.3.

If it is unlikely that a subsequent course in coding theory will be taught, the material in Chapter 7 can be replaced by the last two sections of Chapter 5. This material will show how a compact disc is encoded and decoded, presenting a nice real-world application that students can relate to.

For subsequent semesters of coding theory, we suggest a combination of some of the following blocks of material. With each block we have included sections that will hopefully make the blocks self-contained under the assumption that the first course given above has been completed. Certainly other blocks are possible. A semester can be made up of more than one block. Later we give individual chapters or sections that stand alone and can be used in conjunction with each other or with some of these blocks. The sections and chapters are listed in the order they should be covered.

- Sections 1.7, 8.1–8.4, 9.1–9.7, and Chapter 10. Sections 8.1–8.4 of this block present the essential material relating block designs to codes with particular emphasis on designs arising from self-dual codes. The material from Chapter 9 gives an in-depth study of self-dual codes with connections to designs. Chapter 10 studies the Golay codes and hexacode in great detail, again using designs to help in the analysis. Section 2.11 can be added to this block as the binary Golay codes are lexicodes.
- Sections 1.7, 7.4–7.10, Chapters 8, 9, and 10, and Section 2.11. This is an extension of the above block with more on designs from codes and codes from designs. It also looks at weight distributions in more depth, part of which is required in Section 9.12. Codes closely related to self-dual codes are also examined. This block may require an entire semester.
- Sections 4.6, 5.4.3, 5.4.4, 5.5, 5.6, and Chapters 14 and 15. This block covers most of the decoding algorithms described in the text but not studied in the first course, including both hard and soft decision decoding. It also introduces the important classes of convolutional and turbo codes that are used in many applications particularly in deep space communication. This would be an excellent block for engineering students or others interested in applications.
- Sections 2.2, 2.3, 2.5, 2.6, 2.10, and Chapter 13. This block finishes the nonasymptotic bounds not covered in the first course and presents the asymptotic versions of these bounds. The algebraic geometry codes and Goppa codes are important for, among other reasons, their relationship to the bounds on families of codes.
- Section 1.7 and Chapters 6 and 12. This block studies two families of codes extensively: duadic codes, which include quadratic residue codes, and linear codes over $\mathbb{Z}_4$. There is some overlap between the two chapters to warrant studying them together. When presenting Section 12.5.1, ideas from Section 9.6 should be discussed. Similarly it is helpful to examine Section 10.6 before presenting Section 12.5.3.

The following mini-blocks and chapters could be used in conjunction with one another or with the above blocks to construct a one-semester course.

- Section 1.7 and Chapter 6. Chapter 6 can stand alone after Section 1.7 is covered.
- Sections 1.7, 8.1–8.4, Chapter 10, and Section 2.11. This mini-block gives an in-depth study of the Golay codes and hexacode with the prerequisite material on designs covered first.
- Section 1.7 and Chapter 12. After Section 1.7 is covered, Chapter 12 can be used alone with the exception of Sections 12.4 and 12.5. Section 12.4 can either be omitted or supplemented with material from Section 6.6. Section 12.5 can either be skipped or supplemented with material from Sections 9.6 and 10.6.
- Chapter 11. This chapter can stand alone.
- Chapter 14. This chapter can stand alone.

The authors would like to thank a number of people for their advice and suggestions for this book. Philippe Gaborit tested portions of the text in its earliest form in a coding theory course he taught at the University of Illinois at Chicago resulting in many helpful insights. Philippe also provided some of the data used in the tables in Chapter 6. Judy Walker's monograph [343] on algebraic geometry codes was invaluable when we wrote Chapter 13; Judy kindly read this chapter and offered many helpful suggestions. Ian Blake and Frank Kschischang read and critiqued Chapters 14 and 15 providing valuable direction. Bob McEliece provided data for some of the figures in Chapter 15. The authors also wish to thank the staff and associates of Cambridge University Press for their valuable assistance with production of this book. In particular we thank editorial manager Dr. Philip Meyler, copy editor Dr. Lesley J. Thomas, and production editor Ms. Lucille Murby. Finally, the authors would like to thank their students in coding theory courses whose questions and comments helped refine the text. In particular Jon Lark Kim at the University of Illinois at Chicago and Robyn Canning at Loyola University of Chicago were most helpful.

We have taken great care to read and reread the text, check the examples, and work the exercises in an attempt to eliminate errors. As with all texts, errors are still likely to exist. The authors welcome corrections to any that the readers find. We can be reached at our e-mail addresses below.

W. Cary Huffman
wch@math.luc.edu

Vera Pless
pless@math.uic.edu

February 1, 2003