

Introduction to Coding Theory

Error-correcting codes constitute one of the key ingredients in achieving the high degree of reliability required in modern data transmission and storage systems. This book introduces the reader to the theoretical foundations of error-correcting codes, with an emphasis on Reed–Solomon codes and their derivative codes.

After reviewing linear codes and finite fields, the author describes Reed–Solomon codes and various decoding algorithms. Cyclic codes are presented, as are MDS codes, graph codes, and codes in the Lee metric. Concatenated, trellis, and convolutional codes are also discussed in detail. Homework exercises introduce additional concepts such as Reed–Muller codes, and burst error correction. The end-of-chapter notes often deal with algorithmic issues, such as the time complexity of computational problems.

While mathematical rigor is maintained, the text is designed to be accessible to a broad readership, including students of computer science, electrical engineering, and mathematics, from senior-undergraduate to graduate level.

This book contains over 100 worked examples and over 340 exercises—many with hints.

RON M. ROTH joined the faculty of Technion—Israel Institute of Technology (Haifa, Israel) in 1988, where he is a Professor of Computer Science and holds the General Yaakov Dori Chair in Engineering. He also held visiting positions at IBM Research Division (San Jose, California) and, since 1993, at Hewlett–Packard Laboratories (Palo Alto, California). He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE).

Cambridge University Press
978-0-521-84504-5 - Introduction to Coding Theory
Ron M. Roth
Frontmatter
[More information](#)

Cambridge University Press
978-0-521-84504-5 - Introduction to Coding Theory
Ron M. Roth
Frontmatter
[More information](#)

Introduction to Coding Theory

Ron M. Roth

**Technion—Israel Institute of Technology
Haifa, Israel**



Cambridge University Press
978-0-521-84504-5 - Introduction to Coding Theory
Ron M. Roth
Frontmatter
[More information](#)

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Mexico City

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/9780521845045

© Cambridge University Press 2006

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without the written
permission of Cambridge University Press.

First published 2006
Reprinted with corrections 2007

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

ISBN 978-0-521-84504-5 Hardback

Cambridge University Press has no responsibility for the persistence or
accuracy of URLs for external or third-party internet websites referred to in
this publication, and does not guarantee that any content on such websites is,
or will remain, accurate or appropriate. Information regarding prices, travel
timetables, and other factual information given in this work is correct at
the time of first printing but Cambridge University Press does not guarantee
the accuracy of such information thereafter.

Contents

Preface	page ix
1 Introduction	1
1.1 Communication systems	1
1.2 Channel coding	3
1.3 Block codes	5
1.4 Decoding	7
1.5 Levels of error handling	11
Problems	17
Notes	22
2 Linear Codes	26
2.1 Definition	26
2.2 Encoding of linear codes	28
2.3 Parity-check matrix	29
2.4 Decoding of linear codes	32
Problems	36
Notes	47
3 Introduction to Finite Fields	50
3.1 Prime fields	50
3.2 Polynomials	51
3.3 Extension fields	56
3.4 Roots of polynomials	59
3.5 Primitive elements	60
3.6 Field characteristic	62
3.7 Splitting field	64
3.8 Application: double error-correcting codes	66
Problems	70
Notes	90

4	Bounds on the Parameters of Codes	93
4.1	The Singleton bound	94
4.2	The sphere-packing bound	95
4.3	The Gilbert–Varshamov bound	97
4.4	MacWilliams’ identities	99
4.5	Asymptotic bounds	104
4.6	Converse Coding Theorem	110
4.7	Coding Theorem	115
	Problems	119
	Notes	136
5	Reed–Solomon and Related Codes	147
5.1	Generalized Reed–Solomon codes	148
5.2	Conventional Reed–Solomon codes	151
5.3	Encoding of RS codes	152
5.4	Concatenated codes	154
5.5	Alternant codes	157
5.6	BCH codes	162
	Problems	163
	Notes	177
6	Decoding of Reed–Solomon Codes	183
6.1	Introduction	183
6.2	Syndrome computation	184
6.3	Key equation of GRS decoding	185
6.4	Solving the key equation by Euclid’s algorithm	191
6.5	Finding the error values	194
6.6	Summary of the GRS decoding algorithm	195
6.7	The Berlekamp–Massey algorithm	197
	Problems	204
	Notes	215
7	Structure of Finite Fields	218
7.1	Minimal polynomials	218
7.2	Enumeration of irreducible polynomials	224
7.3	Isomorphism of finite fields	227
7.4	Primitive polynomials	227
7.5	Cyclotomic cosets	229
	Problems	232
	Notes	240

<i>Contents</i>	vii
8 Cyclic Codes	242
8.1 Definition	242
8.2 Generator polynomial and check polynomial	244
8.3 Roots of a cyclic code	247
8.4 BCH codes as cyclic codes	250
8.5 The BCH bound	253
Problems	256
Notes	265
9 List Decoding of Reed–Solomon Codes	266
9.1 List decoding	267
9.2 Bivariate polynomials	268
9.3 GRS decoding through bivariate polynomials	269
9.4 Sudan’s algorithm	271
9.5 The Guruswami–Sudan algorithm	276
9.6 List decoding of alternant codes	280
9.7 Finding linear bivariate factors	284
9.8 Bounds on the decoding radius	289
Problems	291
Notes	295
10 Codes in the Lee Metric	298
10.1 Lee weight and Lee distance	298
10.2 Newton’s identities	300
10.3 Lee-metric alternant codes and GRS codes	302
10.4 Decoding alternant codes in the Lee metric	306
10.5 Decoding GRS codes in the Lee metric	312
10.6 Berlekamp codes	314
10.7 Bounds for codes in the Lee metric	316
Problems	321
Notes	327
11 MDS Codes	333
11.1 Definition revisited	333
11.2 GRS codes and their extensions	335
11.3 Bounds on the length of linear MDS codes	338
11.4 GRS codes and the MDS conjecture	342
11.5 Uniqueness of certain MDS codes	347
Problems	351
Notes	361

12 Concatenated Codes	365
12.1 Definition revisited	366
12.2 Decoding of concatenated codes	367
12.3 The Zyablov bound	371
12.4 Justesen codes	374
12.5 Concatenated codes that attain capacity	378
Problems	381
Notes	392
13 Graph Codes	395
13.1 Basic concepts from graph theory	396
13.2 Regular graphs	401
13.3 Graph expansion	402
13.4 Expanders from codes	406
13.5 Ramanujan graphs	409
13.6 Codes from expanders	411
13.7 Iterative decoding of graph codes	414
13.8 Graph codes in concatenated schemes	420
Problems	426
Notes	445
14 Trellis and Convolutional Codes	452
14.1 Labeled directed graphs	453
14.2 Trellis codes	460
14.3 Decoding of trellis codes	466
14.4 Linear finite-state machines	471
14.5 Convolutional codes	477
14.6 Encoding of convolutional codes	479
14.7 Decoding of convolutional codes	485
14.8 Non-catastrophic generator matrices	495
Problems	501
Notes	518
Appendix: Basics in Modern Algebra	521
Problems	522
Bibliography	527
List of Symbols	553
Index	559

Preface

Do ye imagine to reprove words?
Job 6:26

This book has evolved from lecture notes that I have been using for an introductory course on coding theory in the Computer Science Department at Technion. The course deals with the basics of the theory of error-correcting codes, and is intended for students in the graduate and upper-undergraduate levels from Computer Science, Electrical Engineering, and Mathematics. The material of this course is covered by the first eight chapters of this book, excluding Sections 4.4–4.7 and 6.7. Prior knowledge in probability, linear algebra, modern algebra, and discrete mathematics is assumed. On the other hand, all the required material on finite fields is an integral part of the course. The remaining parts of this book can form the basis of a second, advanced-level course.

There are many textbooks on the subject of error-correcting codes, some of which are listed next: Berlekamp [36], Blahut [46], Blake and Mullin [49], Lin and Costello [230], MacWilliams and Sloane [249], McEliece [259], Peterson and Weldon [278], and Pless [280]. These are excellent sources, which served as very useful references when compiling this book. The two volumes of the *Handbook of Coding Theory* [281] form an extensive encyclopedic collection of what is known in the area of coding theory.

One feature that probably distinguishes this book from most other classical textbooks on coding theory is that generalized Reed–Solomon (GRS) codes are treated *before* BCH codes—and even before cyclic codes. The purpose of this was to bring the reader to see, as early as possible, families of codes that cover a wide range of minimum distances. In fact, the cyclic properties of (conventional) Reed–Solomon codes are immaterial for their distance properties and may only obscure the underlying principles of the decoding algorithms of these codes. Furthermore, bit-error-correcting codes, such as binary BCH codes, are found primarily in spatial communication applications, while readers are now increasingly exposed to temporal com-

munication platforms, such as magnetic and optical storage media. And in those applications—including domestic CD and DVD—the use of GRS codes prevails.

Therefore, the treatment of finite fields in this book is split, where the first batch of properties (in Chapter 3) is aimed at laying the basic background on finite fields that is sufficient to define GRS codes and understand their decoding algorithm. A second batch of properties of finite fields is provided in Chapter 7, prior to discussing cyclic codes, and only then is the reader presented with the notions of minimal polynomials and cyclotomic cosets.

Combinatorial bounds on the parameters of codes are treated mainly in Chapter 4. In an introductory course, it would suffice to include only the Singleton and sphere-packing bounds (and possibly the non-asymptotic version of the Gilbert–Varshamov bound). The remaining parts of this chapter contain the asymptotic versions of the combinatorial bounds, yet also cover the information-theoretic bounds, namely, the Shannon Coding Theorem and Converse Coding Theorem for the q -ary symmetric channel. The latter topics may be deferred to an advanced-level course.

GRS codes and alternant codes constitute the center pillar of this book, and a great portion of the text is devoted to their study. These codes are formally introduced in Chapter 5, following brief previews in Sections 3.8 and 4.1. Classical methods for GRS decoding are described in Chapter 6, whereas Chapter 9 is devoted to the list decoding of GRS codes and alternant codes. The performance of these codes as Lee-metric codes is then the main topic of Chapter 10. GRS codes play a significant role also in Chapter 11, which deals with MDS codes.

The last three chapters of the book focus on compound constructions of codes. Concatenated codes and expander-based codes (which are, in a way, two related topics) are presented in Chapters 12 and 13, and an introduction to trellis codes and convolutional codes is given in Chapter 14. This last chapter was included in this book for the sake of an attempt for completeness: knowing that the scope of the book could not possibly allow it to touch all the aspects of trellis codes and convolutional codes, the model of state-dependent coding, which these codes represent, was still too important to be omitted.

Each chapter ends with problems and notes, which occupy on average a significant portion of the chapter. Many of the problems introduce additional concepts that are not covered in text; these include Reed–Muller codes, product codes and array codes, burst error correction, interleaving, the implementation of arithmetic in finite fields, or certain bounds—e.g., the Griesmer and Plotkin bounds. The notes provide pointers to references and further reading. Since the text is intended also for readers who are computer scientists, the notes often contain algorithmic issues, such as the time com-

plexity of certain computational problems that are related to the discussion in the text.

Finally, the Appendix (including the problems therein) contains a short summary of several terms from modern algebra and discrete mathematics, as these terms are frequently used in the book. This appendix is meant merely to recapitulate material, which the reader is assumed to be rather familiar with from prior studies.

I would like to thank the many students and colleagues, whose input on earlier versions of this book greatly helped in improving the presentation. Special thanks are due to Shirley Halevy, Ronny Lempel, Gitit Ruckenstein, and Ido Tal, who taught the course with me at Technion and offered a wide variety of useful ideas while the book was being written. Ido was particularly helpful in detecting and correcting many of the errors in earlier drafts of the text (obviously, the responsibility for all remaining errors is totally mine). I owe thanks to Brian Marcus and Gadiel Seroussi for the good advice that they provided along the way, and to Gadiel, Vitaly Skachek, and the anonymous reviewers for the constructive comments and suggestions. Part of the book was written while I was visiting the Information Theory Research Group at Hewlett-Packard Laboratories in Palo Alto, California. I wish to thank the Labs for their kind hospitality, and the group members in particular for offering a very encouraging and stimulating environment.

Cambridge University Press
978-0-521-84504-5 - Introduction to Coding Theory
Ron M. Roth
Frontmatter
[More information](#)
