

Cambridge University Press
978-0-521-52923-5 - Coding Theory: A First Course
San Ling and Chaoping Xing
Frontmatter
[More information](#)

Coding Theory

A First Course

Coding theory is concerned with successfully transmitting data through a noisy channel and correcting errors in corrupted messages. It is of central importance for many applications in computer science or engineering. This book gives a comprehensive introduction to coding theory whilst only assuming basic linear algebra. It contains a detailed and rigorous introduction to the theory of block codes and moves on to more advanced topics such as BCH codes, Goppa codes and Sudan's algorithm for list decoding. The issues of bounds and decoding, essential to the design of good codes, feature prominently.

The authors of this book have, for several years, successfully taught a course on coding theory to students at the National University of Singapore. This book is based on their experiences and provides a thoroughly modern introduction to the subject. There is a wealth of examples and exercises, some of which introduce students to novel or more advanced material.

Cambridge University Press
978-0-521-52923-5 - Coding Theory: A First Course
San Ling and Chaoping Xing
Frontmatter
[More information](#)

Coding Theory

A First Course

SAN LING
CHAOPING XING
National University of Singapore



Cambridge University Press
978-0-521-52923-5 - Coding Theory: A First Course
San Ling and Chaoping Xing
Frontmatter
[More information](#)

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa
<http://www.cambridge.org>

© Cambridge University Press 2004

This book 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 2004

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 10/13 pt. *System* L^AT_EX 2_ε [TB]

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

ISBN 0 521 82191 6 hardback
ISBN 0 521 52923 9 paperback

The publisher has used its best endeavours to ensure that the
URLs for external websites referred to in this book are correct and
active at the time of going to press. However, the publisher has no
responsibility for the websites, and can make no guarantee that a
site will remain live or that the content is or will remain appropriate.

Cambridge University Press
978-0-521-52923-5 - Coding Theory: A First Course
San Ling and Chaoping Xing
Frontmatter
[More information](#)

To Mom and Dad
and my beloved wife Bee Keow

S. L.

To my wife Youqun Shi
and my children Zhengrong and Menghong

C. P. X.

Contents

<i>Preface</i>	<i>page xi</i>
1 Introduction	1
Exercises	4
2 Error detection, correction and decoding	5
2.1 Communication channels	5
2.2 Maximum likelihood decoding	8
2.3 Hamming distance	8
2.4 Nearest neighbour/minimum distance decoding	10
2.5 Distance of a code	11
Exercises	14
3 Finite fields	17
3.1 Fields	17
3.2 Polynomial rings	22
3.3 Structure of finite fields	26
3.4 Minimal polynomials	30
Exercises	36
4 Linear codes	39
4.1 Vector spaces over finite fields	39
4.2 Linear codes	45
4.3 Hamming weight	46
4.4 Bases for linear codes	48
4.5 Generator matrix and parity-check matrix	52
4.6 Equivalence of linear codes	56
4.7 Encoding with a linear code	57
4.8 Decoding of linear codes	59

4.8.1 Cosets	59
4.8.2 Nearest neighbour decoding for linear codes	61
4.8.3 Syndrome decoding	62
Exercises	66
5 Bounds in coding theory	75
5.1 The main coding theory problem	75
5.2 Lower bounds	80
5.2.1 Sphere-covering bound	80
5.2.2 Gilbert–Varshamov bound	82
5.3 Hamming bound and perfect codes	83
5.3.1 Binary Hamming codes	84
5.3.2 q -ary Hamming codes	87
5.3.3 Golay codes	88
5.3.4 Some remarks on perfect codes	92
5.4 Singleton bound and MDS codes	92
5.5 Plotkin bound	95
5.6 Nonlinear codes	96
5.6.1 Hadamard matrix codes	98
5.6.2 Nordstrom–Robinson code	98
5.6.3 Preparata codes	99
5.6.4 Kerdock codes	99
5.7 Griesmer bound	100
5.8 Linear programming bound	102
Exercises	106
6 Constructions of linear codes	113
6.1 Propagation rules	113
6.2 Reed–Muller codes	118
6.3 Subfield codes	121
Exercises	126
7 Cyclic codes	133
7.1 Definitions	133
7.2 Generator polynomials	136
7.3 Generator and parity-check matrices	141
7.4 Decoding of cyclic codes	145
7.5 Burst-error-correcting codes	150
Exercises	153

Contents

ix

8	Some special cyclic codes	159
8.1	BCH codes	159
8.1.1	Definitions	159
8.1.2	Parameters of BCH codes	161
8.1.3	Decoding of BCH codes	168
8.2	Reed–Solomon codes	171
8.3	Quadratic-residue codes	175
	Exercises	183
9	Goppa codes	189
9.1	Generalized Reed–Solomon codes	189
9.2	Alternant codes	192
9.3	Goppa codes	196
9.4	Sudan decoding for generalized RS codes	202
9.4.1	Generation of the (\mathcal{P}, k, t) -polynomial	203
9.4.2	Factorization of the (\mathcal{P}, k, t) -polynomial	205
	Exercises	209
	<i>References</i>	215
	<i>Bibliography</i>	217
	<i>Index</i>	219

Preface

In the seminal paper ‘A mathematical theory of communication’ published in 1948, Claude Shannon showed that, given a noisy communication channel, there is a number, called the capacity of the channel, such that reliable communication can be achieved at any rate below the channel capacity, if proper encoding and decoding techniques are used. This marked the birth of coding theory, a field of study concerned with the transmission of data across noisy channels and the recovery of corrupted messages.

In barely more than half a century, coding theory has seen phenomenal growth. It has found widespread application in areas ranging from communication systems, to compact disc players, to storage technology. In the effort to find good codes for practical purposes, researchers have moved beyond block codes to other paradigms, such as convolutional codes, turbo codes, space-time codes, low-density-parity-check (LDPC) codes and even quantum codes. While the problems in coding theory often arise from engineering applications, it is fascinating to note the crucial role played by mathematics in the development of the field. The importance of algebra, combinatorics and geometry in coding theory is a commonly acknowledged fact, with many deep mathematical results being used in elegant ways in the advancement of coding theory.

Coding theory therefore appeals not just to engineers and computer scientists, but also to mathematicians. It has become increasingly common to find the subject taught as part of undergraduate or graduate curricula in mathematics.

This book grew out of two one-semester courses we have taught at the National University of Singapore to advanced mathematics and computer science undergraduates over a number of years. Given the vastness of the subject, we have chosen to restrict our attention to block codes, with the aim of introducing the theory without a prerequisite in algebra. The only mathematical prerequisite assumed is familiarity with basic notions and results in

linear algebra. The results on finite fields needed in the book are covered in Chapter 3.

The design of good codes, from both the theoretical and practical points of view, is a very important problem in coding theory. General bounds on the parameters of codes are often used as benchmarks to determine how good a given code is, while, from the practical perspective, a code must admit an efficient decoding scheme before it can be considered useful. Since the beginning of coding theory, researchers have done much work in these directions and, in the process, have constructed many interesting families of codes. This book is built pretty much around these themes. A fairly detailed discussion on some well known bounds is included in Chapter 5, while quite a number of decoding techniques are discussed throughout this book. An effort is also made to introduce systematically many of the well known families of codes, for example, Hamming codes, Golay codes, Reed–Muller codes, cyclic codes, BCH codes, Reed–Solomon codes, alternant codes, Goppa codes, etc.

In order to stay sufficiently focused and to keep the book within a manageable size, we have to omit certain well established topics or examples, such as a thorough treatment of weight enumerators, from our discussion. Wherever possible, we try to include some of these omitted topics in the exercises at the end of each chapter. More than 250 problems have been included to help strengthen the reader's understanding and to serve as an additional source of examples and results.

Finally, it is a pleasure for us to acknowledge the help we have received while writing this book. Our research work in coding theory has received generous financial assistance from the Ministry of Education (Singapore), the National University of Singapore, the Defence Science and Technology Agency (Singapore) and the Chinese Academy of Sciences. We are thankful to these organizations for their support. We thank those who have read through the drafts carefully and provided us with invaluable feedback, especially Fangwei Fu, Wilfried Meidl, Harald Niederreiter, Yuansheng Tang (who has also offered us generous help in the preparation of Section 9.4), Arne Winterhof and Sze Ling Yeo, as well as the students in the classes MA3218 and MA4261. David Chew has been most helpful in assisting us with problems concerning \LaTeX , and we are most grateful for his help. We would also like to thank Shanthy d/o Devadas for secretarial help.