A Student's Guide to Coding and Information Theory

This easy-to-read guide provides a concise introduction to the engineering background of modern communication systems, from mobile phones to data compression and storage. Background mathematics and specific engineering techniques are kept to a minimum, so that only a basic knowledge of high-school mathematics is needed to understand the material covered. The authors begin with many practical applications in coding, including the repetition code, the Hamming code, and the Huffman code. They then explain the corresponding information theory, from entropy and mutual information to channel capacity and the information transmission theorem. Finally, they provide insights into the connections between coding theory and other fields. Many worked examples are given throughout the book, using practical applications to illustrate theoretical definitions. Exercises are also included, enabling readers to double-check what they have learned and gain glimpses into more advanced topics, making this perfect for anyone who needs a quick introduction to the subject.

STEFAN M. MOSER is an Associate Professor in the Department of Electrical Engineering at the National Chiao Tung University (NCTU), Hsinchu, Taiwan, where he has worked since 2005. He has received many awards for his work and teaching, including the Best Paper Award for Young Scholars by the IEEE Communications Society and IT Society (Taipei/Tainan Chapters) in 2009, the NCTU Excellent Teaching Award, and the NCTU Outstanding Mentoring Award (both in 2007).

PO-NING CHEN is a Professor in the Department of Electrical Engineering at the National Chiao Tung University (NCTU). Amongst his awards, he has received the 2000 Young Scholar Paper Award from Academia Sinica. He was also selected as the Outstanding Tutor Teacher of NCTU in 2002, and he received the Distinguished Teaching Award from the College of Electrical and Computer Engineering in 2003.

A Student's Guide to Coding and Information Theory

STEFAN M. MOSER

PO-NING CHEN

National Chiao Tung University (NCTU),
Hsinchu, Taiwan

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, 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/9781107015838

First published 2012

Printed in the United Kingdom at the University Press, Cambridge

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

ISBN 978-1-107-01583-8 Hardback
ISBN 978-1-107-60196-3 Paperback

Additional resources for this publication at www.cambridge.org/moser

Contents

Contributors

Po-Ning Chen	(Chapter 7)
Francis Lu	(Chapter 3 and 8)
Stefan M. Moser	(Chapter 4 and 5)
Chung-Hsuan Wang	(Chapter 1 and 2)
Jwo-Yuh Wu	(Chapter 6)

Preface

Most of the books on coding and information theory are prepared for those who already have good background knowledge in probability and random processes. It is therefore hard to find a ready-to-use textbook in these two subjects suitable for engineering students at the freshmen level, or for non-engineering major students who are interested in knowing, at least conceptually, how information is encoded and decoded in practice and the theories behind it. Since communications has become a part of modern life, such knowledge is more and more of practical significance. For this reason, when our school requested us to offer a preliminary course in coding and information theory for students who do not have any engineering background, we saw this as an opportunity and initiated the plan to write a textbook.

In preparing this material, we hope that, in addition to the aforementioned purpose, the book can also serve as a beginner's guide that inspires and attracts students to enter this interesting area. The material covered in this book has been carefully selected to keep the amount of background mathematics and electrical engineering to a minimum. At most, simple calculus plus a little probability theory are used here, and anything beyond that is developed as needed. Its first version has been used as a textbook in the 2009 summer freshmen course *Conversion Between Information and Codes: A Historical View* at National Chiao Tung University, Taiwan. The course was attended by 47 students, including 12 from departments other than electrical engineering. Encouraged by the positive feedback from the students, the book went into a round of revision that took many of the students' comments into account. A preliminary version of this revision was again the basis of the corresponding 2010 summer freshmen course, which this time was attended by 51 students from ten different departments. Specific credit must be given to Professor Chung-Hsuan Wang, who volunteered to teach these 2009 and 2010 courses and whose input considerably improved the first version, to Ms. Hui-Ting

Chang (a graduate student in our institute), who has redrawn all the figures and brought them into shape, and to Pei-Yu Shih (a post-doc in our institute) and Ting-Yi Wu (a second-year Ph.D. student in our institute), who checked the readability and feasibility of all exercises. The authors also gratefully acknowledge the support from our department, which continues to promote this course.

Among the eight chapters in this book, Chapters 1 to 4 discuss coding techniques (including error-detecting and error-correcting codes), followed by a briefing in information theory in Chapters 5 and 6. By adopting this arrangement, students can build up some background knowledge on coding through concrete examples before plunging into information theory. Chapter 7 concludes the quest on information theory by introducing the Information Transmission Theorem. It attempts to explain the practical meaning of the so-called *Shannon limit* in communications, and reviews the historical breakthrough of turbo coding, which, after 50 years of research efforts, finally managed to approach this limit. The final chapter takes a few glances at unexpected relations between coding theory and other fields. This chapter is less important for an understanding of the basic principles, and is more an attempt to broaden the view on coding and information theory.

In summary, Chapter 1 gives an overview of this book, including the system model, some basic operations of information processing, and illustrations of how an information source is encoded.

Chapter 2 looks at ways of encoding source symbols such that any errors, up to a given level, can be detected at the receiver end. Basics of modular arithmetic that will be used in the analysis of the error-detecting capability are also included and discussed.

Chapter 3 introduces the fundamental concepts of error-correcting codes using the three-times repetition code and the Hamming code as starting examples. The error-detecting and -correcting capabilities of general linear block codes are also discussed.

Chapter 4 looks at data compression. It shows how source codes represent the output of an information source efficiently. The chapter uses Professor James L. Massey's beautifully simple and elegant approach based on trees. By this means it is possible to prove all main results in an intuitive fashion that relies on graphical explanations and requires no abstract math.

Chapter 5 presents a basic introduction to information theory and its main quantity *entropy*, and then demonstrates its relation to the source coding of Chapter 4. Since the basic definition of entropy and some of its properties are rather dry mathematical derivations, some time is spent on motivating the definitions. The proofs of the fundamental source coding results are then again

based on trees and are therefore scarcely abstract in spite of their theoretical importance.

Chapter 6 addresses how to convey information reliably over a noisy communication channel. The *mutual information* between channel input and output is defined and then used to quantify the maximal amount of information that can get through a channel (the so-called *channel capacity*). The issue of how to achieve channel capacity via proper selection of the input is also discussed.

Chapter 7 begins with the introduction of the Information Transmission Theorem over communication channels corrupted by additive white Gaussian noise. The optimal error rate that has been proven to be attainable by Claude E. Shannon (baptized the *Shannon limit*) is then addressed, particularly for the situation when the amount of transmitted information is above the channel capacity. The chapter ends with a simple illustration of turbo coding, which is considered the first practical design approaching the Shannon limit.

Chapter 8 describes two particularly interesting connections between coding theory and seemingly unrelated fields: firstly the relation of the Hamming code to projective geometry is discussed, and secondly an application of codes to game theory is given.

The title, *A Student's Guide to Coding and Information Theory*, expresses our hope that this book is suitable as a beginner's guide, giving an overview to anyone who wishes to enter this area. In order not to scare the students (especially those without an engineering background), no problems are given at the end of each chapter as usual textbooks do. Instead, the problems are incorporated into the main text in the form of Exercises. The readers are encouraged to work them out. They are very helpful in understanding the concepts and are motivating examples for the theories covered in this book at a more advanced level.

The book will undergo further revisions as long as the course continues to be delivered. If a reader would like to provide comments or correct typos and errors, please email any of the authors. We will appreciate it very much!