MODERN CODING THEORY

Iterative techniques have revolutionized the theory and practice of coding and have been adopted in the majority of next-generation communications standards. *Modern Coding Theory* summarizes the state of the art in iterative coding, with particular emphasis on the underlying theory. Starting with Gallager's original ensemble of low-density parity-check codes as a representative example, focus is placed on the techniques to analyze and design practical iterative coding systems. The basic concepts are then extended for several general codes, including the practically important class of turbo codes. This book takes advantage of the simplicity of the binary erasure channel to develop analytical techniques and intuition, which are then applied to general channel models. A chapter on factor graphs helps to unify the important topics of information theory, coding, and communication theory.

Covering the most recent advances in the field, this book is a valuable resource for graduate students in electrical engineering and computer science, as well as practitioners who need to decide which coding scheme to employ, how to design a new scheme, or how to improve an existing system.

Additional resources, including instructor's solutions and figures, are available online: www.cambridge.org/9780521852296.

Tom Richardson received his Ph.D. in electrical engineering from Massachusetts Institute of Technology in 1990. For ten years, until 2000, he was a member of Bell Labs' Mathematical Sciences Research Center. In 2000, he joined Flarion Technologies, a wireless startup, which was acquired by Qualcomm, Inc. in 2006. He is currently an associate editor for the *IEEE Transactions on Information Theory.*

Rüdiger Urbanke is a professor in the School of Computer and Communication Sciences at EPFL, Switzerland. He was awarded his Ph.D. in electrical engineering in 1995 from Washington University, after which he worked at Bell Labs' Mathematical Sciences Research Center until joining the faculty at Ecole Polytechnique Fédérale de Lausanne in 1999.

Modern Coding Theory

TOM RICHARDSON
Qualcomm, Inc.

RÜDIGER URBANKE
Ecole Polytechnique Fédérale de Lausanne

CAMBRIDGE
UNIVERSITY PRESS

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

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521852296

First published 2008

Printed in the United States of America

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

Library of Congress Cataloging in Publication Data

Richardson, Thomas J. (Thomas Joseph), 1961–
Modern coding theory / By T. Richardson and R. Urbanke.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-521-85229-6 (hardback)
1. Coding theory. I. Urbanke, R. (Rüdiger), 1966– II. Title.
QA268.R53 2008
003′.54–dc22 2007039544

ISBN 978-0-521-85229-6 hardback

To Karen,
Grammel, and Mathilde

CONTENTS

PREFACE

This book is all about *iterative* channel decoding. Two other names which are often used to identify the same area are *probabilistic* coding and *codes on graphs*. Iterative decoding was originally conceived by Gallager in his remarkable Ph.D. thesis of 1960. Gallager's work was, evidently, far ahead of its time. Limitations in computational resources in the 1960s were such that the power of his approach could not be fully demonstrated, let alone developed. Consequently, iterative decoding attracted only passing interest and slipped into a long dormancy. It was rediscovered by Berrou, Glavieux, and Thitimajshima in 1993 in the form of turbo codes, and then independently in the mid 1990s by MacKay and Neal, Sipser and Spielman, as well as Luby, Mitzenmacher, Shokrollahi, Spielman, and Stemann in a form much closer to Gallager's original construction. Iterative techniques have subsequently had a strong impact on coding theory and practice and, more generally, on the whole of communications.

The title *Modern Coding Theory* is clearly a hyperbole. There have been several other important recent developments in coding theory. To mention one prominent example: Sudan's algorithm and the Guruswami-Sudan improvement for list decoding of Reed-Solomon codes and their extension to soft-decision decoding have sparked new life into this otherwise mature subject. So what is our excuse? Iterative methods and their theory are strongly tied to advances in current computing technology and they are therefore inherently modern. They have also brought about a break with the past. Moreover, the techniques are influencing a wide range of applications within and beyond communications, connecting that area with many modern topics in, among others, statistical mechanics and complexity theory. Nevertheless, the font on the book cover expresses the irony that the roots of "modern" coding go back to a time when typewriters ruled the world.

The field of iterative decoding has not settled in the same way that classical coding has. There are nearly as many flavors of iterative decoding systems – and graphical models to represent them – as there are researchers in the field. We have therefore decided to focus more on techniques to analyze and design such systems rather than on specific instances. In order to present the theory, we have elected Gallager's original ensemble of low-density parity-check (LDPC) codes as a representative example. This ensemble is perhaps the most elegant example and it provides a framework within which the main results can be presented easily. Once the basic concepts are absorbed, their extensions to more general cases is typically routine and several such extensions (but not an exhaustive list) are discussed. In particular, we have included a thorough investigation of turbo codes.

A noticeable feature of this book is that we spend a considerable number of pages discussing iterative decoding over the binary erasure channel. Why spend so much time on a very specific and limited channel model? It is probably fair to say that what we now know about iterative decoding we learned first for the binary erasure channel. The basic analysis of iterative coding in the context of the binary erasure channel needs little more than pen and paper and some knowledge of calculus and probability. Nearly all important concepts developed during the study of the binary erasure channel carry over to general channels, although our current ability to extend the results is, in some cases, frustrated by technical challenges.

This book is written with several audiences in mind. First, we hope that it will be a useful text for a course in coding theory. If such a course is dedicated solely to iterative techniques, most necessary material should be contained in this book. If the course covers both classical algebraic coding and iterative topics, this book can be used in conjunction with one of the many excellent books on classical coding. We have intentionally excluded virtually all classical material, except for the most basic definitions. Second, we hope that this book will also be of use to the practitioner in the field who is trying to design or choose a coding scheme for a new communication system or to improve an existing system. Third, we hope that the book will serve as a useful reference for researchers in the field.

There are many possible paths through this book. Our own personal preference is to start with the chapter on factor graphs (Chapter 2). The material covered in this chapter has the special appeal that it unifies many themes of information theory, coding, and communication. Although all three areas trace their origin to Shannon's 1948 paper, they have subsequently diverged and specialized to a point where a typical textbook in one area treats each of the other two topics as distant cousins and gives them just passing reference. The factor graph approach is a nice way to glue them back together. The same technique allows for the computation of capacity, and deals with equalization, modulation, and coding on an equal footing. Following Chapter 2, we recommend covering the core of the material in Chapter 3 (binary erasure channel) and Chapter 4 (general binary memoryless symmetric channels) in a linear fashion.

The remaining material can be read in almost any order according to the preferences of the reader. One may choose to broaden the view and to go through some of the material on more general channels (Chapter 5). Alternatively, you might be more interested in general ensembles. Chapter 6 discusses turbo codes and Chapter 7 deals with various further ensembles and some issues of graph design.

Chapter 8 gives a brief look at a complementary way of analyzing iterative systems in terms of the expansion of the underlying bipartite graph. These techniques are usually aimed at proving guaranteed error-correcting capability and are usually not capable of predicting typical error-correcting performance.

The Appendices contain various chapters on topics which either describe tools for analysis or are simply too technical to fit into the main part. Appendix A takes a look at the encoding problem. Curiously, for iterative schemes the encoding task can be of equal (or even higher) complexity than the decoding task. Appendix B discusses efficient and accurate ways of implementing density evolution. In Appendix C we describe various techniques from probability which are useful in asserting that most elements of a properly chosen ensemble behave "close" to the ensemble average. We take a close look at generating functions in Appendix D. In particular we discuss how to accurately estimate the coefficients of powers of polynomials – a recurrent theme in this book. Finally, in Appendix E we collected a few proofs deemed too lengthy to include in the main text.

Although we have tried to make the material as accessible as possible, the prerequisites for different portions of the book vary considerably. Some seemingly simple issues require sophisticated tools for their resolution. A good example is the material related to the weight distribution of LDPC codes. When the density of equations increases to a painful level, the casual reader is advised not to get discouraged but rather to skip the proofs. Fortunately, in all these cases the subsequent material depends very little on the mathematical details of the proof.

If you are a lecturer and you are giving a beginning graduate-level course we recommend that you follow the basic course outlined above but skip some of the less accessible topics. For general binary memoryless symmetric channels one can first focus on Gallager's decoding algorithm A. The analysis for this case is very similar to the one for the binary erasure channel. A subsequent discussion of the belief propagation decoder can skip some of the proofs and so avoid a discussion of some of the technical difficulties. If your course is positioned as an advanced graduate-level course then most of the material should be accessible to the students.

We intended to write a thin book containing all there is to know about iterative decoding. We ended up with a rather thick one with a number of regrettable omissions: We do not cover the emerging theory of pseudo codewords and their connections to the error floor for general channels and we only scratched the surface of the rich area of interleaver design. The theory of rateless codes is deserving of a much more detailed look. We have not discussed the powerful techniques borrowed from statistical mechanics, which have been used successfully in the analysis of iterative systems. Finally, we mention, but do not discuss, source coding by iterative techniques.

Even within the topics we have covered many interesting extensions and details have been set aside and not been included. For these shortcomings, to paraphrase Descartes, "[We] hope that posterity will judge [us] kindly, not only as to the things which [we] have explained, but also as to those which [we] have intentionally omitted so as to leave to others the pleasure of discovery." ;-)

We have received much help over the years. We would like to thank A. Ahmed, A. Amraoui, B. Bauer, J. Boutros, S.-Y. Chung, H. Croonie, C. Di, N. Dütsch, J. Ezri, T. Filler, W. H. Fong, M. P. C. Fossorier, A. Guillen i Fabregas, M. Haenggi, T. Hehn, D. Huang, A. Karbasi, B. Konsbruck, S. Korada, S. Kudekar, L. Gong, N. Macris, A. Orlitsky, H. D. Pfister, D. Porrat, V. Rathi, K. S. Reddy, V. Skachek, A. Shokrollahi, D. A. Spielman, I. Tal, A. J. van Wijngaarden, L. Varshney, P. O. Vontobel, X. Wang, G. Wiechman, and L. Zhichu for providing us with feedback, and we apologize to all of those whom we missed.

Special thanks go to A. Barg, C. Berrou, M. Durvy, G. D. Forney, Jr., G. Kramer, D. J. C. MacKay, C. Méasson, S. S. Pietrobon, B. Rimoldi, D. Saad, E. Telatar, and Y. Yu for their extensive reviews and the large number of suggestions they provided. Probably nobody read the initial manuscript more carefully and provided us with more feedback than Igal Sason. We are very thankful to him for this invaluable help.

A. Chebira, J. Ezri, A. Gueye, T. Ktari, C. Méasson, C. Neuberg, and P. Reymond were of tremendous help in producing the figures and simulations. Thank you for all the work you did.

A considerable portion of this book is the direct result of our various collaborations. We enjoyed working with A. Amraoui, L. Bazzi, S.-Y. Chung, C. Di, S. Dusad, J. Ezri, G. D. Forney, Jr., H. Jin, N. Kahale, N. Macris, C. Méasson, A. Montanari, V. Novichkov, H. D. Pfister, D. Proietti, V. Rathi, A. Shokrollahi, I. Sason, and E. Telatar on many topics related to this book.

Nobody has contributed more to the realization of this book than E. Telatar (a.k.a. "Emre the Wise"). He hand-picked the font (MinionPro), designed the layout (using the "memoir" package by P. Wilson), showed us how to program figures in PostScript by hand, was our last resort for any LaTeX questions, and generously provided his expertise and advice in many other areas.

This book would not have been finished without the constant encouragement by P. Meyler at Cambridge. We thank A. Littlewood at Cambridge and P. Rote at Aptara for their expert handling.

Last but not least, M. Bardet has managed to keep the chaos at bay at EPFL despite RU's best efforts to the contrary. I would like to thank her for this miraculous accomplishment.

The idea for this book was born at the end of the last millennium when we were both happy members of the Mathematics of Communications group at Bell Labs headed by the late A. D. Wyner and then by J. Mazo. We would like to thank both of them for giving us the freedom to pursue our ideas. Since our departure from Bell Labs, EPFL and Flarion Technologies/Qualcomm have been our hospitable homes.

T. Richardson
South Orange, NJ

R. Urbanke
Lausanne, Switzerland
November, 2007