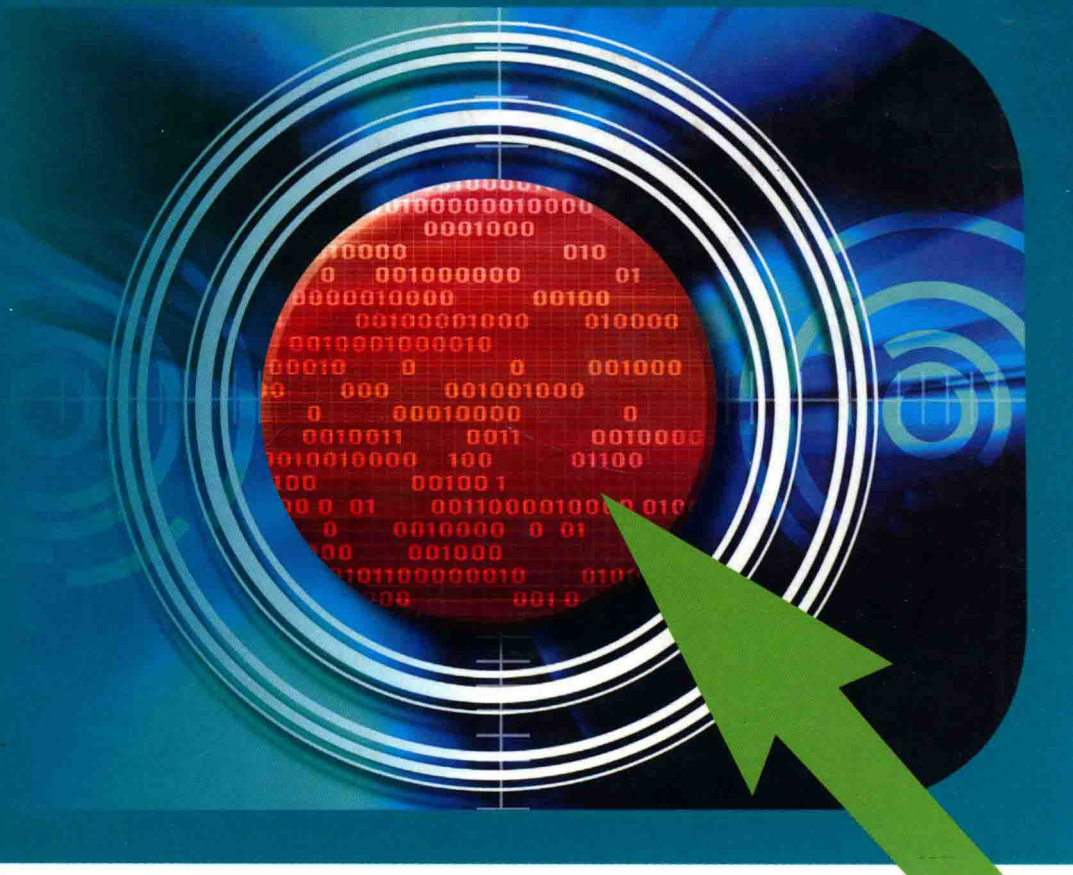
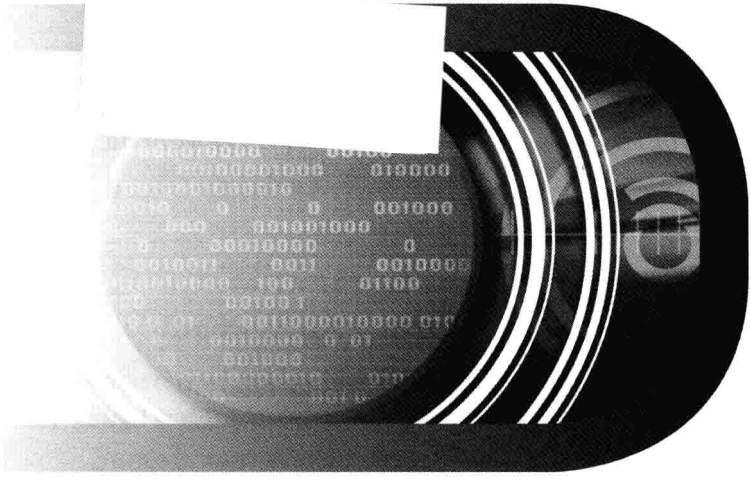
Series on Coding Theory and Cryptology – Vol. 7



Editors
I. Woungang
S. Misra
S. C. Misra

SELECTED TOPICS IN INFORMATION AND CODING THEORY

Series on Coding Theory and Cryptology – Vol. 7



SELECTED TOPICS IN INFORMATION AND CODING THEORY

Editors

I. Woungang
Ryerson University, Canada

S. Misra
Indian Institute of Technology, Kharagpur, India

S. C. Misra
State University of New York at Buffalo, USA

World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

SELECTED TOPICS IN INFORMATION AND CODING THEORY
Series on Coding Theory and Cryptology — Vol. 7

ISBN-13 978-981-283-716-5
ISBN-10 981-283-716-7

Typeset by Stallion Press
Email: enquiries@stallionpress.com

Printed in Singapore by Mainland Press Pte Ltd.

SELECTED TOPICS IN INFORMATION AND CODING THEORY

Series on Coding Theory and Cryptology

Editors: Harald Niederreiter *(National University of Singapore, Singapore)* and San Ling *(Nanyang Technological University, Singapore)*

Published

Vol. 1 Basics of Contemporary Cryptography for IT Practitioners
by B. Ryabko and A. Fionov

Vol. 2 Codes for Error Detection
by T. Kløve

Vol. 3 Advances in Coding Theory and Cryptography
eds. T. Shaska et al.

Vol. 4 Coding and Cryptology
eds. Yongqing Li et al.

Vol. 5 Advances in Algebraic Geometry Codes
eds. E. Martínez-Moro, C. Munuera and D. Ruano

Vol. 6 Codes over Rings
ed. P. Solé

Vol. 7 Selected Topics in Information and Coding Theory
eds. I. Woungang, S. Misra and S. Chandra Misra

Dedicated to

Isaac's wife: Clarisse and sons: Clyde, Lenny, Kylian
Subhas's daughter: Devarati
Sudip's son: Devadeep

PREFACE

Overview and Goals

Information and Coding Theory research and applications are undergoing rapid advancements. The last few years have witnessed rapid advancements in Information and Coding Theory research and applications. This book provides a comprehensive guide to selected topics, both ongoing and emerging, in Information and Coding Theory. Consisting of contributions from well known and high profile researchers in their respective specialties, topics that are covered include applications of coding theory to computational complexity, algebraic combinatorics in coding theory, codes construction and existence, source coding, channel capacity, network coding, and few other selected topics in Information and Coding Theory research.

The book has been prepared keeping in mind that it needs to prove itself to be a valuable resource dealing with both the important core and the specialized issues in Information and Coding Theory. We hope that it will be a valuable reference for students, instructors, researchers, engineers, and industry practitioners in these fields. All of the chapters are integrated in a manner that renders the book as a supplementary reference volume and/or textbook for use in both undergraduate and graduate courses on Information and Coding Theory. Each chapter is of an expository, but also of a scholarly, tutorial, or survey style, on a particular topic within the scope of Information and Coding Theory.

Organization and Features

The book is organized into 15 chapters, each chapter written by topical area experts. These chapters are grouped into four parts.

Part 1 is devoted to the applications of coding theory to computational complexity, and is composed of three chapters: Chaps. 1–3. Chapter 1 discusses several theoretical methods for analyzing the linear complexity and related complexity measures and proposes several classes of interesting sequences with high linear complexity. Chapter 2 focuses on the construction of high coding gain lattices with low decoding complexity from good codes in larger dimensions, and proposes a possible lattice construction with high coding gain using turbo codes and Low Density Parity Check codes. Chapter 3 is dedicated to the issues of cooperative communication in wireless relay networks. Various constructions of the distributed space-time block codes with low maximum-likelihood decidability are surveyed, and new upper bounds on the maximum rate of certain classes of single-symbol decodable distributed space-time block codes are proposed.

Part 2 focuses on methods of algebraic combinatorics in coding theory, and methods of codes construction and existence. It is composed of four chapters: Chaps. 4–7. Chapter 4 discusses in-depth the interplay of coding theory and algebraic combinatorics, focusing on the interaction of codes with combinatorial designs. Chapter 5 discusses ways and results in which to define, construct, prove theorems, and analyze codes from group rings in general, using both zero-divisor and units within a group ring. The codes derived are described as either zero-divisor or unit-derived codes. Chapter 6 is a continuation of the work initiated in Chapter 5, by presenting a new algebraic group ring-based method for constructing codes with no short cycles in the check matrix, and a general algebraic method for constructing Low Density Parity Check codes with no short cycles. Chapter 7 presents the construction of some well-known classes of algebraic block codes, and discusses recent generalizations of quasi-cyclic codes, as well as some algebraic and combinatorial methods of obtaining new codes from existing ones.

Part 3 centers on source coding, channel capacity, and network coding issues. It is composed of three chapters: Chaps. 8–10. Chapter 8 introduces a new approach to estimation, prediction and hypothesis testing for time series based on ideas of universal coding or universal data compression. Chapter 9 presents a subjective approach to network coding, which is concerned with the deterministic multicast encoding of cyclic networks. This topic is presented at a level of detail that is not found elsewhere in the literature. Chapter 10 addresses the problem of transmission of several distributed sources over a multiple access channel with side information

at the sources and the decoder, and proposes a joint source channel coding approach, which generalizes previous results available on the studied problem.

Part 4 addresses other selected topics in Information and Coding Theory, and is composed of five chapters; Chaps. 11–15. Chapter 11 presents a tutorial exposition of Low Density Parity Check codes. Chapter 12 focuses on some selected topics in the theory of variable length codes, including connections with codes for constrained channels and sources. Chapter 13 deals with decoding techniques and methods for finding the minimum distance of linear codes by means of Gröbner bases. Chapter 14 presents an overview of cooperative diversity, along with latest advances and open issues in this evolving field. In Chap. 15, algebraic coding theory is used as an alternative way to define secure cryptographic primitives.

We list below some of the important features of this book, which, we believe, would make it a valuable resource for our readers:

- This book is designed, in structure and content, to aid the learning process with the intention of making the book useful at all learning levels.
- Most of the chapters of the book are authored by prominent academicians/researchers, practitioners, in Information and Coding Theory that have been working with these topics for quite a few years now and have thorough understanding of the concepts.
- The authors of this book are distributed in a large number of countries and most of them are affiliated with institutions of worldwide repute. This gives this book an international flavor.
- Most of the chapters in this book have a distinct section providing direction for future research, which, particularly, targets researchers working in these areas. We believe that this section should provide insight to the researchers about some of the current research issues.
- The authors of each chapter have attempted to provide a comprehensive bibliography, which should greatly help the readers interested further to dig into the topics.
- Most of the chapters of this book have a separate section outlining thoughts for practitioners. We believe that this section in every chapter will be particularly useful for industry practitioners working directly with the practical aspects behind enabling these technologies in the field.
- All chapters, except one, provide a set of questions at the end that can help in assessing the understanding of the readers. In most chapters, solutions are provided to some of these questions.

- To make the book useful for pedagogical purposes, all chapters of the book have a corresponding set of presentation slides. The slides can be obtained as a supplementary resource by contacting the publisher, World Scientific, Singapore.

We have made attempts in all possible ways we could to make the different chapters of the book look as much coherent and synchronized as possible. However, it cannot be denied that due to the fact chapters were written by different authors, it was not fully possible to fully achieve this task. We believe that this is a limitation of most edited books of this sort.

Target Audience

The book is written by primarily targeting the student community. This includes the students of all levels — those getting introduced to these areas, those having an intermediate level of knowledge of the topics, and those who are already knowledgeable about many of the topics. To keep up with this goal, we have attempted to design the overall structure and content of the book in such a manner that makes it useful at all learning levels. To aid in the learning process, almost all chapters have a *set of questions* at the end of the chapter. Also, in order that teachers can use this book for classroom teaching, the book also comes with *presentation slides* and *sample solutions* to exercise questions, which are available as supplementary resources.

The secondary audience for this book is the research community, whether they are working in the academia or in the industry. To meet the specific needs to this audience group, certain chapters of the book provide directions for future research.

Finally, we have also taken into consideration the needs to those readers, typically from the industries, who have quest for getting insight into the practical significance of the topics, i.e. how the spectrum of knowledge and the ideas are relevant for real-life applications of coding and information theory.

Supplementary Resources

As mentioned earlier, the book comes with *presentation slides* for each chapter, which can be used for classroom instruction by teachers.

Teachers can contact the publisher, World Scientific, Singapore, to get access to these resources.

Acknowledgments

We are extremely thankful to the 25 authors of the 15 chapters of this book, who have worked very hard to bring this unique resource forward for help of the student, researcher, and practitioner community. The authors were very much interactive at all stages of preparation of the book from initial development of concept to finalization. We feel it is contextual to mention that as the individual chapters of this book are written by different authors, the responsibility of the contents of each of the chapters lies with the concerned authors.

We are also very much thankful to our colleagues in the World Scientific publishing and marketing teams, in particular, Ms. Kimberly Chua, Ms. Chelsea Chin, and Ms. Mei Kian, who tirelessly worked with us and guided us in the publication process. Special thanks also go to them for taking special interest in publishing this book, considering the current worldwide market needs for such a book.

Finally, we would like to thank our parents, Mr. J. Sime, Ms. C. Seupa, Prof. J.C. Misra, Ms. Shorasi Misra, our wives Clarisse, Satamita, and Sulagna, and our children Clyde, Lenny, Kylian, Babai, and Tultuli, for the continuous support and encouragement they offered during the course of this project.

Dr. Isaac Woungang
Toronto, ON, Canada

Dr. Subhas Chandra Misra
Kanpur, UP, India

Dr. Sudip Misra
Kharagpur, WB, India

CONTRIBUTORS

Nuh Aydin
Department of Mathematics
Kenyon College, Gambier, OH 43022, USA
aydinn@kenyon.edu

Tsvetan Asamov
Department of Mathematics
Kenyon College, Gambier, OH 43022, USA
asamovt@kenyon.edu

Marie-Pierre Béal
Institut Gaspard-Monge (IGM)
Université Paris-Est
77454 Marne-la-Vallée Cedex 2, Paris, France
beal@univ-mlv.fr

Jean Berstel
Institut Gaspard-Monge (IGM), Université Paris-Est
77454 Marne-la-Vallée Cedex 2, Paris, France
berstel@univ-mlv.fr

Dominique Perrin
Institut Gaspard-Monge (IGM)
Université Paris-Est
77454 Marne-la-Vallée Cedex 2, Paris, France
dominique.perrin@esiee.fr

Brian H. Marcus
University of British Columbia
B.C., Vancouver, Canada
marcus@math.ubc.ca

Christophe Reutenauer
LaCIM, Université du Québec à Montréal
Montréal, Canada
reutenauer.christophe@uqam.ca

Paul H. Siegel
Department of Electrical and Computer Engineering
University of California at San Diego, San Diego, USA
psiegel@ucsd.edu

Boris Ryabko
Siberian State University of Telecommunications
and Informatics and Institute of Computational Technology
of Siberian Branch of Russian Academy of Science, Russia
boris@ryabko.net

Stanislav Bulygin
Department of Mathematics
University of Kaiserslautern
P.O. Box 3049, 67653 Kaiserslautern, Germany
bulygin@mathematik.uni-kl.de

Ruud Pellikaan
Department of Mathematics and Computing Science
Eindhoven University of Technology, P.O. Box 513
NL-5600 MB, Eindhoven, The Netherlands
g.r.pellikaan@tue.nl

Michael Huber
Institut für Mathematik, Technische Universität Berlin,
Straße des 17. Juni 136, D-10623, Berlin, Germany
mhuber@math.TU-Berlin.DE

Murat Uysal
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada, N2L3G1
muysal@ece.uwaterloo.ca

Muhammad Mehboob Fareed
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
mmfareed@ece.uwaterloo.ca

Angela I. Barbero
Department of Applied Mathematics
University of Valladolid
47011 Valladolid, Spain
angbar@wmatem.eis.uva.es

Oyvind Ytrehus
Department of Informatics
University of Bergen, N-5020 Bergen, Norway
oyvind@ii.uib.no

G. Susinder Rajan
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012, India
susinder@ece.iisc.ernet.in

B. Sundar Rajan
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012, India
bsrajan@ece.iisc.ernet.in

Mohammd-Reza Sadeghi
Faculty of Mathematics and Computer Science
Amirkabir University of Technology Hafez Ave.
Tehran, Iran
msadeghi@aut.ac.ir

Vinod Sharma
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012, India
vinod@ece.iisc.ernet.in

R. Rajesh
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012, India
rajesh@pal.ece.iisc.ernet.in

Paul Hurley
IBM Research
Zurich Research Laboratory, Switzerland
pah@zurich.ibm.com

Ted Hurley
Department of Mathematics
National University of Ireland
Galway, Ireland
ted.hurley@nuigalway.ie

Pascal Véron
Institut de Mathématiques de Toulon
Université du Sud Toulon-Var
Toulon, France
veron@univ-tln.fr

Xudong Ma
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo
Ontario N2L 3G1, Canada
x3ma@bbcr.uwaterloo.cay

CONTENTS