Codes, Cryptology and Curves with Computer Algebra

Ruud Pellikaan, Xin-Wen Wu,
Stanislav Bulygin and Relinde Jurrius

This well-balanced text touches on theoretical and applied aspects of protecting digital data. The reader is provided with the basic theory and is then shown deeper fascinating detail, including the current state of the art. Readers will soon become familiar with methods of protecting digital data while it is transmitted, as well as while the data is being stored.

Both basic and advanced error-correcting codes are introduced together with numerous results on their parameters and properties. The authors explain how to apply these codes to symmetric and public key cryptosystems and secret sharing. Interesting approaches based on polynomial systems solving are applied to cryptography and decoding codes. Computer algebra systems are also used to provide an understanding of how objects introduced in the book are constructed, and how their properties can be examined. This book is designed for Masters-level students studying mathematics, computer science, electrical engineering or physics.

RUUD PELLIKAAN has tenure at the Technische Universiteit Eindhoven, The Netherlands where his research has shifted from a devotion to coding theory, particularly algebraic geometry codes and their decoding, to code-based cryptography. He previously served as an associate editor of the *IEEE Transactions of Information Theory* and has organised several conferences.

XIN-WEN WU is a Senior Lecturer at the School of Information and Communication Technology, Griffith University, Australia. His research interests include coding theory and information theory, cyber and data security, applied cryptography, communications and networks. He has published extensively in these areas and is a senior member of the Institute of Electrical and Electronics Engineers (IEEE).

STANISLAV BULYGIN works as a technology specialist and product manager in the field of IT security and banking services. He previously worked as a researcher focusing on cryptology and IT security at the Technical University of Darmstadt, Germany. His main research activities were connected to the theory of error-correcting codes and their use in cryptography, quantum resistant cryptosystems and algebraic methods in cryptology.

RELINDE JURRIUS is an Assistant Professor at the Université de Neuchâtel, Switzerland. Her research interests are in coding theory, network coding and its connection with other branches of mathematics such as matroid theory, algebraic and finite geometry, and combinatorics. Apart from research and teaching, she is active in organizing outreach activities, including a math camp for high school students, a public open day for the Faculty of Science and extra-curricular activities for elementary school children.

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org

ISBN 978-0-521-52036-2

COVER DESIGNED BY HART McLEOD LTD

Pellikaan, Wu, Bulygin and Jurrius

Codes, Cryptology and Curves with Computer Algebra

CAMBRIDGE

Codes, Cryptology and Curves with Computer Algebra

RUUD PELLIKAAN
Technische Universiteit Eindhoven, The Netherlands

XIN-WEN WU
Griffith University, Australia

STANISLAV BULYGIN

RELINDE JURRIUS
Université de Neuchâtel, Switzerland

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

4843/24, 2nd Floor, Ansari Road, Daryaganj, Delhi – 110002, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521817110
DOI: 10.1017/9780511982170

First published 2018

Printed in the United Kingdom by Clays, St Ives plc

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

ISBN 978-0-521-81711-0 Hardback
ISBN 978-0-521-52036-2 Paperback

Codes, Cryptology and Curves with Computer Algebra

This well-balanced text touches on theoretical and applied aspects of protecting digital data. The reader is provided with the basic theory and is then shown deeper fascinating detail, including the current state of the art. Readers will soon become familiar with methods of protecting digital data while it is transmitted, as well as while the data is being stored.

Both basic and advanced error-correcting codes are introduced together with numerous results on their parameters and properties. The authors explain how to apply these codes to symmetric and public key cryptosystems and secret sharing. Interesting approaches based on polynomial systems solving are applied to cryptography and decoding codes. Computer algebra systems are also used to provide an understanding of how objects introduced in the book are constructed, and how their properties can be examined. This book is designed for Masters-level students studying mathematics, computer science, electrical engineering or physics.

RUUD PELLIKAAN has tenure at the Technische Universiteit Eindhoven, The Netherlands where his research has shifted from a devotion to coding theory, particularly algebraic geometry codes and their decoding, to code-based cryptography. He previously served as an associate editor of the *IEEE Transactions of Information Theory* and has organised several conferences.

XIN-WEN WU is a Senior Lecturer at the School of Information and Communication Technology, Griffith University, Australia. His research interests include coding theory and information theory, cyber and data security, applied cryptography, communications and networks. He has published extensively in these areas and is a senior member of the Institute of Electrical and Electronics Engineers (IEEE).

STANISLAV BULYGIN works as a technology specialist and product manager in the field of IT security and banking services. He previously worked as a researcher focusing on cryptology and IT security at the Technical University of Darmstadt, Germany. His main research activities were connected to the theory of error-correcting codes and their use in cryptography, quantum resistant cryptosystems and algebraic methods in cryptology.

RELINDE JURRIUS is an Assistant Professor at the Université de Neuchâtel, Switzerland. Her research interests are in coding theory, network coding and its connection with other branches of mathematics such as matroid theory, algebraic and finite geometry, and combinatorics. Apart from research and teaching, she is active in organizing outreach activities, including a math camp for high school students, a public open day for the Faculty of Science and extra-curricular activities for elementary school children.

If three men be walking together,
and (only) one of them be under a delusion,
they may yet reach their goal, the deluded being the fewer;
but if two of them be under the delusion, they will not do so,
the deluded being the majority.

"Heaven and Earth" chapter 14
Zhuangzi (370–287 BC) [364]

Preface

An early version of this book was a handwritten manuscript from around 1990. In June 2001 a synopsis was written by invitation of Cambridge University Press with the working title "The construction and decoding of algebraic geometry codes," or "Algebraic geometry and its applications (in error-correcting codes and cryptography)." That proposal was accepted, but with no indication of a deadline. So originally its aim was a book on algebraic geometry codes. As time passed more and more co-authors joined the team: Xin-Wen Wu in 2004, Stanislav Bulygin in 2007 and finally Relinde Jurrius in 2012.

Early versions of chapters were written on algebraic geometry codes, elementary coding theory, list decoding Reed–Muller codes, decoding algorithms and Gröbner bases, cryptography, weight enumerators and its generalizations and relations with matroid theory that appeared in books and journals [68, 69, 70, 71, 177, 184, 186, 266].

The prerequisites of this book are: elementary logical reasoning and naive set theory, some combinatorics and probability theory. Furthermore: linear algebra, the beginnings of group theory, the algebra of rings and fields. We will go into the details of polynomial rings and finite fields in several chapters.

The first six chapters of the book on the construction, properties and decoding of error-correcting codes are self-contained. This can be used as a course in Coding Theory of four hours a week during a semester in the first year of the Masters. It is advised to use Chapter 12 from the start to practise the theory with computer algebra systems.

The second half of the book on complexity theory, cryptology, Gröbner bases applied to codes and cryptosystems and algebraic geometry codes is more advanced. This can be used for a course in the second year of a Masters degree or can be read individually as a Capita Selecta. It is

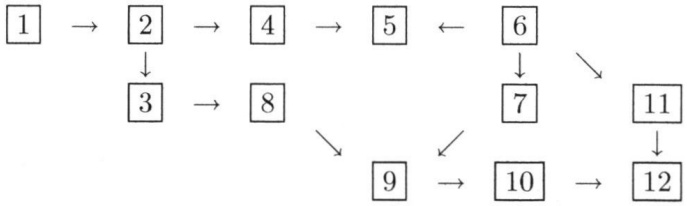
also a good starting point for a project or assignment. In the Notes at the end of every chapter we give ample references to further reading.

We thank the editors of Cambridge University Press: David Tranah, Jonathan Walthoe, Roger Astley, Clare Dennison and Abigail Walkington for their advice and patience.

The logical dependency between the chapters

1 Error-correcting codes
2 Code constructions and bounds
3 Weight enumeration
4 Cyclic codes
5 Polynomial codes
6 Algebraic decoding
7 Complexity and decoding
8 Codes and related structures
9 Cryptology
10 Gröbner bases for coding and cryptology
11 Codes on curves
12 Coding and cryptology with computer algebra

is given in the following diagram:



The authors may be contacted at:

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

x.wu@griffith.edu.au, School of Information and Communication Technology, Gold Coast Campus, Griffith University, QLD 4222, Australia

bulygin5@googlemail.com, Stanislav Bulygin made the lion's share of his contribution while at Technische Universität Kaiserslautern and Technische Universität Darmstadt (both Germany) in 2008–2013

relinde.jurrius@unine.ch, Institut de Mathémathiques, Université de Neuchâtel, Rue Emilie-Argand 11, 2000 Neuchâtel, Switzerland

Contents

1

Error-correcting Codes

Ruud Pellikaan and Xin-Wen Wu

The idea of *redundant* information is a well-known phenomenon in reading a newspaper. Misspellings usually go unnoticed for a casual reader, while the meaning is still grasped. In Semitic languages such as Hebrew, and even older in the hieroglyphics in the tombs of the pharaohs of Egypt, only the consonants are written while the vowels are left out so that we do not know for sure how to pronounce these words nowadays. The letter "e" is the most frequent occurring symbol in the English language, and leaving out all these letters would still give in almost all cases an understandable text to the expense of greater attention of the reader.

The science of deleting redundant information in a clever way such that it can be stored in less memory or space and still can be expanded to the original message is called *data compression* or *source coding*. It is not the topic of this book. So we can compress data, but an error made in a compressed text would give a different message that is most of the time utterly meaningless.

The idea in *error-correcting codes* is the converse. One adds redundant information in such a way that it is possible to detect or even correct errors after transmission. In radio contacts between pilots and radar controls the letters in the alphabet are spoken phonetically as "Alpha, Bravo, Charlie, ..." but "Adams, Boston, Chicago, ..." is more commonly used for spelling in a telephone conversation. The addition of a parity check symbol enables one to detect an error, such as on the former punch cards that were fed into a computer, in the ISBN code for books, the European Article Numbering (EAN) and the Universal Product Code (UPC) for articles. Error-correcting codes are common

in numerous modern applications where data are required to be stored, processed and transmitted in a reliable manner, such as in audiovisual media, quick response (QR) codes, fault-tolerant computer systems and deep space telecommunication, to name but a few.

In this chapter, we present an introduction to error-correcting codes focusing on the most commonly used codes, namely, block codes and linear codes, including fundamental concepts and procedures for code construction, encoding and decoding.

1.1 Block Codes

Legend goes that Hamming was so frustrated the computer halted every time it detected an error after he handed in a stack of punch cards, he thought about a way the computer would be able not only to detect the error but also to correct it automatically. He came up with his nowadays famous code named after him. Whereas the theory of Hamming is about the actual construction, the encoding and decoding of codes and uses tools from *combinatorics* and *algebra*, the approach of Shannon leads to *information theory* and his theorems tell us what is and what is not possible in a *probabilistic* sense.

According to Shannon we have a message $\mathbf{m}$ in a certain alphabet and of a certain length, we encode $\mathbf{m}$ to $\mathbf{c}$ by expanding the length of the message and adding redundant information. One can define the *information rate* R that measures the slowing down of the transmission of the data. The encoded message $\mathbf{c}$ is sent over a noisy channel such that the symbols are changed, according to certain probabilities that are characteristic of the channel. The received word $\mathbf{r}$ is decoded to $\mathbf{m}'$. See Figure 1.1. Now given the characteristics of the channel one can define the *capacity* C of the channel and it has the property that for every $R < C$ it is possible to find an encoding and decoding scheme such that the *error probability* that $\mathbf{m}' \neq \mathbf{m}$ is arbitrarily small. For $R > C$ such

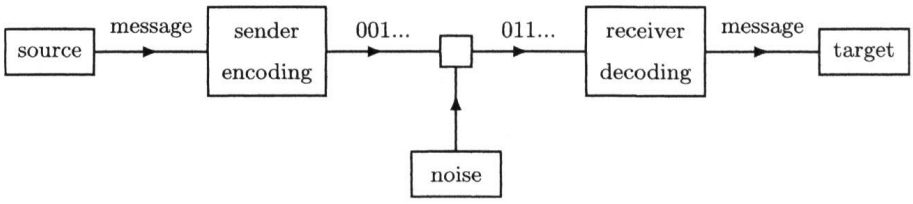


Figure 1.1 Block diagram of a communication system