Springer Undergraduate Mathematics Series

For other titles published in this series, go to
www.springer.com/series/3423

Norman L. Biggs

Codes: An Introduction to Information Communication and Cryptography

Springer

Norman L. Biggs
Department of Mathematics
London School of Economics
Houghton Street
London WC2A 2AE, UK

Springer Undergraduate Mathematics Series ISSN 1615-2085
ISBN: 978-1-84800-272-2 e-ISBN: 978-1-84800-273-9
DOI: 10.1007/978-1-84800-273-9

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

Library of Congress Control Number: 2008930146

Mathematics Subject Classification (2000): 94A, 94B, 11T71

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

Springer Science+Business Media
springer.com

Preface

Many people do not realise that mathematics provides the foundation for the devices we use to handle information in the modern world. Most of those who do know probably think that the parts of mathematics involved are quite 'classical', such as Fourier analysis and differential equations. In fact, a great deal of the mathematical background is part of what used to be called 'pure' mathematics, indicating that it was created in order to deal with problems that originated within mathematics itself. It has taken many years for mathematicians to come to terms with this situation, and some of them are still not entirely happy about it.

This book is an integrated introduction to Coding. By this I mean replacing symbolic information, such as a sequence of bits or a message written in a natural language, by another message using (possibly) different symbols. There are three main reasons for doing this: Economy (data compression), Reliability (correction of errors), and Security (cryptography).

I have tried to cover each of these three areas in sufficient depth so that the reader can grasp the basic problems and go on to more advanced study. The mathematical theory is introduced in a way that enables the basic problems to be stated carefully, but without unnecessary abstraction. The prerequisites (sets and functions, matrices, finite probability) should be familiar to anyone who has taken a standard course in mathematical methods or discrete mathematics. A course in elementary abstract algebra and/or number theory would be helpful, but the book contains the essential facts, and readers without this background should be able to understand what is going on.

There are a few places where reference is made to computer algebra systems. I have tried to avoid making this a prerequisite, but students who have access to such a system will find it helpful. In particular, there are occasional specific references to MAPLE^{TM} (release 10), by Maplesoft, a division of Waterloo Maple Inc., Waterloo, Canada.

The book has been developed from a course of twenty lectures on Information, Communication, and Cryptography given for the MSc in Applicable Mathematics at the London School of Economics. I should like to thank all those students who have contributed to the development of the course materials, in particular those who have written dissertations in this area: Rajni Kanda, Ovijit Paul, Arunduti Dutta-Roy, Ana de Corbavia-Perisic, Raminder Ruprai, James Rees, Elisabeth Biell, Anisa Bhatt, Timothy Morill, Shivam Kumar, and Carey Chua. I owe a special debt to Raminder Ruprai, who worked through all the exercises and helped to sort out many mistakes and obscurities.

Finally, I am grateful to Aaron Wilson, who helped to produce the diagrams, and especially to Karen Borthwick, who has been very helpful and supportive on behalf of the publishers.

Norman Biggs
January 2008

Contents