The Art of Error Correcting Coding

SECOND EDITION

Robert H. Morelos-Zaragoza

Companion Website

WILEY

The Art of Error Correcting Coding

The Art of Error Correcting Coding, Second Edition Robert H. Morelos-Zaragoza
© 2006 John Wiley & Sons, Ltd. ISBN: 0-470-01558-6

The Art of Error Correcting Coding

Second Edition

Robert H. Morelos-Zaragoza
San Jose State University, USA

John Wiley & Sons, Ltd

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wiley.com

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 42 McDougall Street, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 6045 Freemont Blvd, Mississauga, ONT, L5R 4J3, Canada

Wiley also publishes its books in a variety of electronic formats. Some content that appears
in print may not be available in electronic books.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN-13: 978-0-470-01558-2 (HB)
ISBN-10: 0-470-01558-6 (HB)

Typeset in 10/12pt Times by Laserwords Private Limited, Chennai, India.
Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, England.
This book is printed on acid-free paper responsibly manufactured from sustainable forestry
in which at least two trees are planted for each one used for paper production.

Contents

Preface

The first edition of this book was the result of hundreds of emails from all over the world with questions on the theory and applications of error correcting coding (ECC), from colleagues from both academia and industry. Most of the questions have been from engineers and computer scientists needing to select, implement or simulate a particular coding scheme. The questions were sparked by a popular web site[1] initially set up at Imai Laboratory at the Institute of Industrial Science, University of Tokyo, in early 1995. An important aspect of this text is the absence of theorems and proofs. The approach is to teach basic concepts using simple examples. References to theoretical developments are made when needed. This book is intended to be a reference guide to error correcting coding techniques for graduate students and professionals interested in learning the basic techniques and applications of ECC. Computer programs that implement the basic encoding and decoding algorithms of practical coding schemes are available on a companion web site. This site is referred to as the "ECC web site" throughout the text and is located at:

`http://the-art-of-ecc.com`

This book is unique in that it introduces the basic concepts of error correcting codes with simple illustrative examples. Computer programs written in C language and new Matlab[2] scripts are available on the ECC web site and help illustrate the implementation of basic encoding and decoding algorithms of important coding schemes, such as convolutional codes, Hamming codes, BCH codes, Reed–Solomon codes and turbo codes, and their application in digital communication systems. There is a rich theory of ECC that will be touched upon, by referring to the appropriate material. There are many good books dealing with the theory of ECC, for example, references (Lin and Costello 2005), (MacWilliams and Sloane 1977), (Peterson and Weldon 1972), (Blahut 1984), (Bossert 1999), (Wicker 1995), just to cite a few. Readers may wish to consult them before, during or after going through the material in this book. Each chapter describes, using simple and easy-to-follow numerical examples, the basic concepts of a particular coding or decoding scheme, rather than going into the detail of the theory behind it. Basic analysis tools are given to help in the assessment of the error performance of a particular ECC scheme.

The book deals with the *art* of error correcting coding, in the sense that it addresses the need for selecting, implementing and simulating algorithms for encoding and decoding of codes for error correction and detection. New features of the second edition include additional in-text examples as well as new problems at the end of each chapter, intended for use in a course on ECC. A comprehensive bibliography is included, for readers who wish

[1] `http://www.eccpage.com`

[2] Matlab is a registered trademark of The Mathworks, Inc.

to learn more about the beautiful theory that makes it all work. The book is organized as follows. In Chapter 1, the basic concepts of error correction and coding and decoding techniques are introduced. Chapter 2 deals with important and simple-to-understand families of codes, such as the Hamming, Golay and Reed–Muller codes. In Chapter 3, cyclic codes and the important family of BCH codes are described. Finite-field arithmetic is introduced and basic decoding algorithms, such as Berlekamp–Massey, Euclidean and PGZ, are described, and easy to follow examples are given to understand their operation. Chapter 4 deals with Reed–Solomon codes and errors-and-erasures decoding. A comprehensive treatment of the available algorithms is given, along with examples of their operation. In Chapter 5, binary convolutional codes are introduced. Focus in this chapter is on the understanding of the basic structure of these codes, along with a basic explanation of the Viterbi algorithm with Hamming metrics. Important implementation issues are discussed. In Chapter 6, several techniques for modifying a single code or combining several codes are given and illustrated by simple examples. Chapter 7 deals with soft-decision decoding algorithms, some of which have not yet received attention in the literature, such as a soft-output ordered-statistics decoding algorithm. Moreover, Chapter 8 presents a unique treatment of turbo codes, both parallel concatenated and serial concatenated, and block product codes, from a coding theoretical perspective. In the same chapter, low-density parity-check codes are examined. For all these classes of codes, basic decoding algorithms are described and simple examples are given. Finally, Chapter 9 deals with powerful techniques that combine error correcting coding with digital modulation, and several clever decoding techniques are described.

I would like to express my gratitude to the following persons for inspiring this work. Professor Francisco Garcia Ugalde, Universidad Nacional Autónoma de México, for introducing me to the exciting world of error correcting codes. Parts of this book are based on my Bachelor’s thesis under his direction. Professor Edward Bertram, University of Hawaii, for teaching me the basics of abstract algebra. Professor David Muñoz, Instituto Technológico y de Estudios Superiores de Monterrey, México, for his kindness and support. Professors Tadao Kasami, Hiroshima City University, Toru Fujiwara, University of Osaka, and Hideki Imai, University of Tokyo, for supporting my stay as a visiting academic researcher in Japan. Dan Luthi and Advait Mogre, LSI Logic Corporation, for many stimulating discussions and the opportunity to experience the process of putting ideas into silicon. Marc P. C. Fossorier of University of Hawaii for his kind help. My former colleague Dr. Misa Mihaljević of Sony Computer Science Laboratories, for pointing out connections between decoding and cryptoanalysis. I would also like to thank wholeheartedly Dr. Mario Tokoro, President of Sony Computer Science Laboratories, and Professor Ryuji Kohno, Yokohama National University, for making it possible for me to have a fine environment in which to write the first edition of this book. In particular, I want to express my eternal gratitude to Professor Shu Lin of University of California at Davis. I am also grateful to the graduate students of San Jose State University who took my course and helped in designing and testing some of the problems in the second edition.

I dedicate this book to Richard W. Hamming, Claude Shannon and Gustave Solomon, three extraordinary gentlemen who greatly impacted the way people live and work today.

Robert H. Morelos-Zaragoza
San Jose, California, USA