

Applied and Numerical Harmonic Analysis

Series Editor

John J. Benedetto

University of Maryland
College Park, MD, USA

Editorial Advisory Board

Akram Aldroubi

Vanderbilt University
Nashville, TN, USA

Andrea Bertozzi

University of California
Los Angeles, CA, USA

Douglas Cochran

Arizona State University
Phoenix, AZ, USA

Hans G. Feichtinger

University of Vienna
Vienna, Austria

Christopher Heil

Georgia Institute of Technology
Atlanta, GA, USA

Stéphane Jaffard

University of Paris XII
Paris, France

Jelena Kovačević

Carnegie Mellon University
Pittsburgh, PA, USA

Gitta Kutyniok

University of Osnabrück
Osnabrück, Germany

Mauro Maggioni

Duke University
Durham, NC, USA

Zuowei Shen

National University of Singapore
Singapore, Singapore

Thomas Strohmer

University of California
Davis, CA, USA

Yang Wang

Michigan State University
East Lansing, MI, USA

David Joyner • Jon-Lark Kim

Selected
Unsolved
Problems in
Coding Theory

 Birkhäuser

David Joyner
Mathematics Department
US Naval Academy
Chauvenet Hall
Holloway Road 572C
Annapolis, Maryland 21402
USA
wdjoyner@gmail.com

Jon-Lark Kim
Department of Mathematics
University of Louisville
Natural Sciences Building 328
Louisville, KY 40292
USA
jl.kim@louisville.edu

ISBN 978-0-8176-8255-2

e-ISBN 978-0-8176-8256-9

DOI 10.1007/978-0-8176-8256-9

Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2011935547

Mathematics Subject Classification (2010): 94-02, 94B05, 94B25, 94B27, 11T71, 14G50, 05B05, 05B15

© Springer Science+Business Media, LLC 2011

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

www.birkhauser-science.com

Preface

This book is intended for research mathematicians interested in unsolved problems, and graduate students in mathematics or engineering who are interested in the mathematical side of the theory of error-correcting codes. It also may be of interest to coding-theorists who simply want to know how to use SAGE to do certain computations with error-correcting codes.

Strong undergraduates should find much in this book of some interest as well. In terms of classroom use, this text could serve as a basis for a special topics course in the theory of error-correcting codes. A good background in algebra, especially linear algebra, would be needed from the student. Some sections also require a strong background in algebraic geometry and number theory.

Coding theory is the branch of mathematics concerned with reliably transmitting data across noisy channels. In many cases, one can simply subdivide the data stream into blocks of a fixed *length* k and then encode each such block with some redundancy to a “codeword” of longer length n , which is then transmitted. With enough redundancy, the hope is that the receiver can recover the original k data bits. For example, in the late 1960s to early 1970s NASA’s Mariner 9 took pictures¹ of Mars such as in Fig. 1. Black and white images such as in Fig. 1 were transmitted through space back to Earth using the so-called Reed–Muller code of length $n = 32$, with $k = 6$ data bits and $n - k = 26$ redundancy bits.

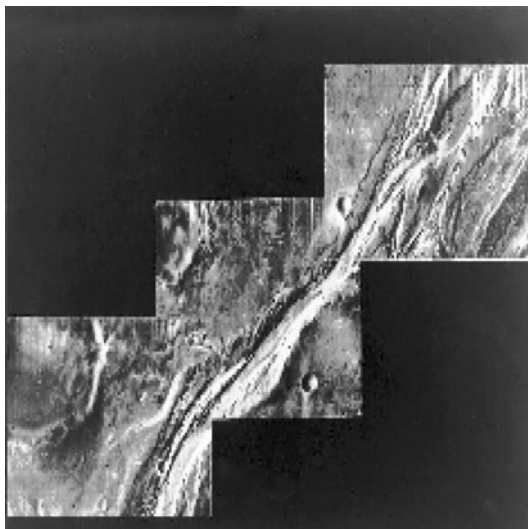
In spite of over 60 years of intensive work from the best minds in the world, there are many interesting mathematical questions which remain unsolved in the theory of error-correcting codes. The modest aim of this book will provide some “publicity” for some of those questions.

A chapter-by-chapter overview follows. We have tried to order the chapters by the rough level of mathematical sophistication required from the reader.

Chapter 1 contains a brief discussion of some basic terms and results on error-correcting codes. For example, the binary symmetric channel, entropy and uncer-

¹This image of Mars’ Olympus Mons was found on the NASA website <http://marsprogram.jpl.nasa.gov/MPF/martianchronicle/martianchron2/index.html> and is in the public domain. See also http://en.wikipedia.org/wiki/Mariner_9.

Fig. 1 Mars' Olympus Mons taken by Mariner 9



tainty, Shannon's theorem, the Hamming metric, the weight distribution (or spectrum) of a code, decoding basics, bounds on the parameters of a code (such as the Singleton bound, Manin's theorem, and the Gilbert–Varshamov asymptotic bound), and examples of important codes such as the Hamming codes and the quadratic residue codes. SAGE examples are scattered throughout to emphasize the computational aspect.

Chapter 2 is a very short chapter surveying certain aspects of the beautiful theory resulting in the intersection between self-dual codes, lattices, and invariant theory. This is a large field with several excellent books and survey articles already written. We introduce weight enumerator polynomials (and the MacWilliams identity), divisible codes and their classification, invariants associated to the different types of self-dual codes arising in this classification, and lattices arising from self-dual codes. The chapter ends with a discussion of the famous unsolved (at present) problem of the existence of a self-dual [72, 36, 16] binary code. Again, some SAGE examples are given. A few proofs are sketched, but most results are stated with only references to original proofs.

Chapter 3 discusses some fascinating results in the intersection between coding theory, block designs, group theory, orthogonal arrays, Latin squares, and recreational mathematics. After introducing Hadamard matrices (and the Hadamard conjecture, with SAGE examples), one of the most remarkable results in all of coding theory is discussed, the Assmus–Mattson theorem. Roughly speaking, this theorem shows a relationship between certain codes and the construction of certain block designs. Connections with Latin squares and orthogonal arrays are given. The unexpected combinatorial structure “hidden” in certain “design-theoretic” codes is exemplified by the constructions in the section involving a Golay code and the “kitten” and “minimog” constructions. The last sections of the chapter discuss recreational aspects of the theory—strategies for winning a “mathematical blackjack” card-game and horsetrack-betting.

Chapter 4 explores an intriguing analogy between the Duursma zeta function (a recently introduced “invariant” object associated to a linear code) and the zeta function attached to an algebraic curve over a finite field. Much remains unknown (at this time) regarding the Duursma zeta function, but this chapter surveys its known properties (mostly with proofs). Several SAGE examples are given; in fact, SAGE is the only mathematics software package (at this time) with commands to compute Duursma zeta functions.

Chapter 5 discusses two very hard and unsolved problems. The first is a nontrivial estimate for the number of solutions (mod p) to a polynomial equation $y^2 = f(x)$, where $f(x)$ is a polynomial whose degree is “small” compared to the prime p . (When p is small compared to the degree of f , then Weil’s estimate gives a good estimate of the number of solutions.) The second unsolved problem is the best asymptotic bounds for a binary linear code. The surprise is that these two seemingly unrelated problems are in fact, rather closely related. Aspects of this relationship, with some proofs and SAGE examples, are discussed in detail.

Finally, Chap. 6 discusses some aspects of algebraic-geometric codes (or AG codes, for short). These are codes arising generally from algebraic varieties over finite fields, though the focus here is on modular curves. This is a relatively technical chapter, requiring some familiarity of number theory, algebraic geometry, and modular forms and also of representation theory of finite groups. Fitting with the general theme of this book, this chapter mostly illustrates how little we know about the algebraic structure of AG codes arising from modular curves. As with many other areas of mathematics, it seems that the more one knows, the more one discovers how little is really known.

Acknowledgements DJ: I thank John Benedetto for the suggestion to write this book and all his encouragement over the years.

JLK: I thank Professor Emeritus Vera Pless of University of Illinois at Chicago for teaching me the insight of coding theory. I also thank my coauthor David Joyner for his encouragement.

For Chap. 3, we thank Alex Ryba and Andy Buchanan for helpful comments, and Ann Casey, who coauthored (with DJ) a much earlier and shorter version.

For Chap. 4, we are grateful to Thann Ward for the reference to [S1], Koji Chinen for many interesting emails about his work, and to Cary Huffman and Iwan Duursma for very interesting conversations on this topic.

For Chap. 5, we thank Prof. Amin Shokrollahi of the Ecole Polytechnique Fédérale de Lausanne for helpful advice and Prof. Felipe Voloch of the University of Texas for allowing his construction to be included above. Parts of this (such as Proposition 156) can be found in the honors thesis [C] of DJ’s former student Greg Coy, who was a pleasure to work with.

Part of Chap. 6 was written with Salahoddin Shokranian of the Universidade de Brasília (and Amin Shokrollahi’s uncle!). Other parts were adapted from a paper written with Amy Ksir (of the US Naval Academy). We also thank D. Prasad and R. Guralnick for enlightening correspondence and in particular for the references [KP] and [Ja1].

Contents

1	Background on Information Theory and Coding Theory	1
1.1	Binary Symmetric Channel	1
1.1.1	Uncertainty	2
1.1.2	Shannon's Theorem	3
1.2	A Simple Example	4
1.3	Basic Definitions	7
1.3.1	The Hamming Metric	9
1.4	Linear Block Codes	10
1.4.1	Decoding Basics	12
1.4.2	Hamming Codes over $GF(q)$	14
1.5	Bounds on the Parameters of a Code	16
1.5.1	Question: What Is "The Best" Code?	18
1.5.2	The Fake Singleton Bound	21
1.6	Quadratic Residue Codes and Other Group Codes	22
1.6.1	Automorphism Groups	22
1.6.2	Cyclic Codes	22
1.6.3	Quadratic Residue Codes	24
2	Self-dual Codes, Lattices, and Invariant Theory	29
2.1	Weight Enumerators	29
2.2	Divisible Codes	31
2.3	Some Invariants	35
2.4	Codes over Other Finite Rings	38
2.5	Lattices from Codes	39
2.5.1	Constructions from Codes	42
2.5.2	Theta Function of a Lattice	43
2.6	More Problems Related to a Prize Problem	44
3	Kittens, Mathematical Blackjack, and Combinatorial Codes	47
3.1	Hadamard Matrices and Codes	47
3.2	Designs, Orthogonal Arrays, Latin Squares, and Codes	51
3.2.1	Examples from Golay Codes	53

3.2.2	Assmus–Mattson Theorem	53
3.2.3	Orthogonal Arrays, Latin Squares and Codes	56
3.3	Curtis’ Kitten, Conway’s Minimog	58
3.3.1	The MINIMOG Description	61
3.3.2	Construction of the Extended Ternary Golay Code	64
3.3.3	The “col/tet” Construction	65
3.3.4	The Kitten Labeling	66
3.4	Playing “Mathematical Blackjack”	67
3.5	Playing the Horses	70
4	The Riemann Hypothesis and Coding Theory	71
4.1	Introduction to the Riemann Zeta Function	72
4.2	Introduction to the Duursma Zeta Function	73
4.3	Introduction	74
4.3.1	Virtual Weight Enumerators	74
4.4	The Zeta Polynomial	77
4.4.1	First Definition	77
4.4.2	Second Definition	83
4.4.3	Third Definition	84
4.4.4	Analogies with Curves	86
4.5	Properties	88
4.5.1	The Functional Equation	89
4.5.2	Puncturing Preserves P	91
4.5.3	The Riemann Hypothesis	91
4.6	Self-reciprocal Polynomials	93
4.6.1	“Smoothness” of Roots	94
4.6.2	Variations on a Theorem of Eneström–Kakeya	94
4.6.3	A Literature Survey	95
4.6.4	Duursma’s Conjecture	103
4.6.5	A Conjecture on Zeros of Cosine Transforms	104
4.7	Examples	106
4.7.1	Komichi’s Example	106
4.7.2	The Extremal Case	107
4.7.3	“Random Divisible Codes”	110
4.7.4	A Formally Self-dual $[26, 13, 6]_2$ -code	110
4.7.5	Extremal Codes of Short Length	111
4.7.6	Non-self-dual Examples	112
4.8	Chinen Zeta Functions	113
4.8.1	Hamming Codes	117
4.8.2	Golay Codes	118
4.8.3	Examples	118
5	Hyperelliptic Curves and Quadratic Residue Codes	123
5.1	Introduction	124
5.2	Points on Hyperelliptic Curves over Finite Fields	124
5.3	Non-Abelian Group Codes	126

- 5.4 Cyclotomic Arithmetic mod 2 126
- 5.5 Quasi-quadratic Residue Codes 128
- 5.6 Weight Distributions 136
- 5.7 Long Quadratic Residue Codes 138
 - 5.7.1 Examples 141
 - 5.7.2 Goppa’s Conjecture Revisited 141
- 5.8 Some Results of Voloch 141
- 6 Codes from Modular Curves 145**
 - 6.1 An Overview 145
 - 6.2 Introduction to Algebraic Geometric Codes 146
 - 6.2.1 The Codes 147
 - 6.2.2 The Projective Line 148
 - 6.3 Introduction to Modular Curves 150
 - 6.3.1 Shimura Curves 151
 - 6.3.2 Hecke Operators and Arithmetic on $X_0(N)$ 157
 - 6.3.3 Eichler–Selberg Trace Formula 159
 - 6.3.4 Modular Curves $X(N)$ 161
 - 6.4 Application to Codes 163
 - 6.4.1 The Curves $X_0(N)$ of Genus 1 167
 - 6.5 Some Estimates on AG Codes 168
 - 6.6 Examples 169
 - 6.6.1 The Generator Matrix (According to Goppa) 170
 - 6.7 Ramification Module of $X(N)$ 172
 - 6.7.1 Example: $N = 7$ 173
- 7 Appendices 177**
 - 7.1 Coding Theory Commands in SAGE 177
 - 7.2 Finite Fields 179
 - 7.3 Tables of Self-dual Codes in SAGE 182
 - 7.4 Proofs 183
 - 7.4.1 MacWilliam’s Identity 183
 - 7.4.2 Mallows–Sloane–Duursma Bounds 185
 - 7.5 Ramification Module and Equivariant Degree 187
- References 189**
- Index 197**