Applied and Numerical Harmonic Analysis

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

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 pictures[1] 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-

[1]This 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.

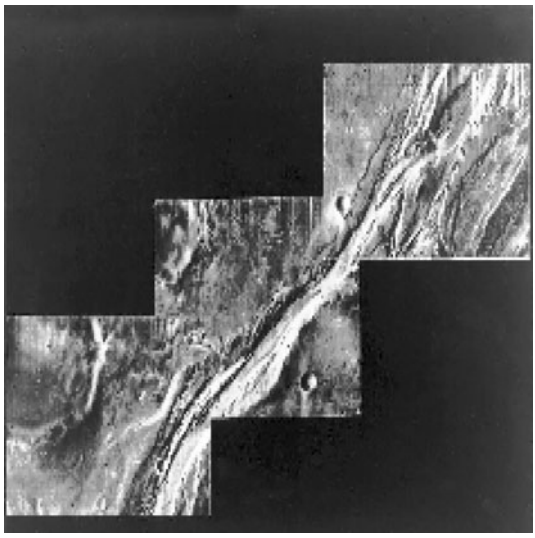

Fig. 1 Mars' Olympus Mons taken by Mariner 9

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 [Sl], 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