Preface

The fascinating theory of error-correcting codes is a rather new addition to the list of mathematical disciplines. It grew out of the need to communicate information electronically, and is currently no more than 60 years old. Being an applied discipline by definition, a surprisingly large number of pure mathematical areas tie into Coding Theory. If one were to name just the most important connections, one would start of course with Linear Algebra, then list Algebra and Combinatorics, and further mention Number Theory and Geometry as well as Algebraic Geometry.

Being a thorough introduction to the field, this book starts from the very beginning, which is the channel model of communication in the presence of noise. From there, we develop the fundamental concepts of error-correcting codes, like the Hamming metric and the maximum likelihood decoding principle. After discussing dual codes and simple decoding procedures, this book takes an unusual turn. The standard approach would be to move on from there and introduce either more theory or present standard constructions of codes. The approach taken here is different.

After raising the question of what it means for codes to be "essentially different" we consider the metric Hamming space together with its isometries, which are the maps preserving the metric structure. This in turn will lead to a rigorous definition of equivalence of codes. In fact, we will call codes isometric if they are equivalent as subspaces of the Hamming space. After that, the discussion shifts to a more abstract analysis of the different kinds of isometries. This is laying out the more general theme behind this book. In essence, this book serves two purposes. On the one hand, the book introduces the fundamentals of the theory of error correcting codes like parameters, bounds as well as known classes of codes including the important class of cyclic codes (Chapters 1–4). Also included is a decent introduction to the theory of finite fields (Chapter 3). Moreover the application of coding theory to CD-players is discussed in detail. On the other hand, the second part of the book covers more advanced and specialized topics which so far have not yet made it into the standard textbooks in the area.

Chapters 1–4 are the core of everyone's understanding of the theory of error correcting codes. Chapter 1 discusses basic concepts, including isometry, weight enumerators, systematic encoding, and a section on the explicit computation of the minimum distance of a code. Chapter 2 is also classic. We discuss bounds on the parameters of codes. This involves both direct combinatorial bounds and also bounds which are obtained from modifications of codes. Particular series of codes are introduced, like the general form of the

Hamming-codes, the extended binary Golay-code of length 24, the class of Reed–Muller-codes as well as a general discussion of MDS-codes.

Chapter 3 is devoted to the theory of finite fields. No book on linear codes can do without such a chapter. Usually, this discussion is placed somewhat after the general introduction of codes and before things get more involved. We have tried to keep the theory of finite fields together in one single chapter, at perhaps the expense of keeping the reader waiting longer than usual. We hope that this decision pays off in that the body of the theory of finite fields can be presented in a single entity. We start with algebraic elements, discuss minimal polynomials, finite field extensions and their automorphisms, i.e. the Galois group. The discussion moves on to finite group actions, and their applications to field theory. Using the notion of Lyndon words, this allows the construction of irreducible polynomials and hence the construction of finite fields of any given order. We discuss two distinct ways of representing field elements on a computer, and the final section is devoted to a brief introduction of the projective geometry over a finite field.

Chapter 4 is dedicated to cyclic codes. The reader will learn about the very important classes of Reed–Solomon and BCH-codes. The close relationship between cyclic codes and ideals in the group algebra is discussed. Furthermore, we discuss quadratic-residue-codes, Golay-codes, idempotent generators and the Fourier Transform, Alternant-codes and Goppa-codes, the structure of cyclic codes as modules, general Reed–Muller-codes, and encoding and decoding issues. It should be noted that Alternant-codes and Goppa-codes are not in general cyclic. The reason for discussing them in the context of cyclic codes is that the algebraic tool of the Chinese Remainder Theorem makes it easy to treat these codes in that context.

Chapter 5 introduces the reader to the application of Coding Theory in connection with the compact disc, a technique which was developed in the early 1980's by the Philips and Sony companies. The reader will see decoding algorithms for BCH-codes, interleaving methods, product codes and an introduction to Fourier analysis and Shannon's Sampling Theorem.

In Chapters 6–9, we start the second part of the above-mentioned division. Here, we come back to the fundamental question "To what extent do good codes exist and how can we find them?" This is of course the fundamental problem of Coding Theory, and in a sense mostly anything studied so far is concerned with certain aspects of this problem. Nevertheless, to answer this question qualitatively, we must go beyond the scope of standard texts. The first step to tackle this problem was made by David Slepian in the 1960's, when he pioneered the application of techniques from Combinatorics to this problem. In fact, he used a technique which is known as Pólya's Theory of Enumeration to the problem of determining the number of isometry classes of codes. In this way, he was able to determine how many classes there are for any given set of parameters. The method involves a fairly detailed study of the way isometries act on the Hamming space. His delicate and powerful computations are brought up again here, and they are refined and adapted to match all different types of isometries we consider. The presentation in Chapter 6 will introduce the reader to this very versatile topic of Combinatorics. At the end, numbers of isometry classes of codes will be presented. This chapter also features sections on random generation of codes, the notion of critical indecomposable codes as introduced by E. Assmus, and a section on the explicit construction of normal bases of finite fields.

After the enumeration of codes, we move on to the construction of representatives of the isometry classes. As a matter of fact, enumeration theory does not tell us about the minimum distance of the codes. For this, we have to construct codes explicitly. There are essentially two different strategies. Both rely on the close connection between codes and geometry, more precisely configurations in finite projective spaces. Each of the two methods allows the restriction to "good" codes, i.e. codes with high minimum distance. This is facilitated by specifying a lower bound on the minimum distance and then constructing only those codes whose minimum distance is bounded below by the given value. In the extreme case, the algorithm would prove that there are no codes with the desired minimum distance.

The first approach (Chapter 8) makes yet another assumption, namely on the presence of symmetries, or – as we shall call them – automorphisms. This is a method which has had its successes recently in other areas, like the theory of combinatorial designs, and it proves to be powerful in that objects can be constructed which would otherwise be out of reach. In fact, the method of lattice actions combined with a construction of configurations called minihypers allows the construction of good codes with a preassigned group of automorphisms. This chapter is based on results of Chapter 7, which discusses lattice methods. A lattice is a set of vectors which are integer linear combinations of a given set of linearly independent vectors in a finite dimensional vector space. These structures are studied in Number Theory. Here, we use lattices to solve integer equations, also known as Diophantine linear equations. Finding the integral solutions of such systems of equations is known to be a very hard problem, since there is no discrete analogue of Gaussian elimination. To solve these systems, combinatorial techniques like lattice basis reduction are applied, combined with enumeration techniques to search through lattices for "short" vectors. As it turns out, the construction problem of codes with preassigned group of automorphisms can be reduced to solving such a system of integer equations, so Chapters 7 and 8 may be considered as a sequence. Several hundred new optimal codes could be constructed with this method which in essence relies on an enormous data reduction because of the group action. That is, the assumption on the existence of nontrivial automorphisms is essential for reducing the size of the problem. On the other hand, the general construction problem (i.e. without making any assumption on the presence of automorphisms) is another topic.

This is where the second method comes in. This time, there will be no further assumption other than the lower bound on the minimum distance. To tackle the "general case" (Chapter 9), a full search on all codes is facilitated, using isomorph rejection in order to construct each isometry class of codes exactly once. This technique searches through the set of all possible codes according to the lexicographical ordering, and is therefore known as orderly generation. In fact, the technique was developed in the 1970's for the construction of graphs, and has since been refined and applied to a plethora of different problems. It was only a matter of time that this technique would find its way to the construction problem of codes. This book will finish with a brief account on the orderly generation of linear codes with a prescribed minimum distance. This involves a fair amount of algorithmic background for dealing with permutation groups. We will present the reader with essential concepts of how to work with permutation groups on a computer and how to solve orbit type problems. We describe in detail the theoretical aspects of dealing with the projective linear and semilinear groups. In the end, we give tables classifying the optimal linear codes for small or moderate parameters over various finite fields.

Chapter A, the appendix, contains an introduction to the attached compact disc. It describes the installation of the software in both a Windows and a Linux environment. It also gives a survey on the accompanying data. The most recently updated version of the programs should be found at the website

http://linearcodes.uni-bayreuth.de

The included software allows one to compute the minimum distance and the weight distribution of given codes, construct codes with a given minimum distance and randomly generate linear codes which are uniformly distributed over the isometry classes of codes with given parameters. The dynamic tables describe the isometry classes of linear codes. In the precomputed tables the reader will find enumerative results on numbers of semilinear isometry classes. Moreover, there are tables containing information on optimal linear codes. The largest possible minimum distance is given, together with the number of semilinear isometry classes of such optimal codes. In addition, corresponding generator matrices can be found. Altogether, around 2 million isometry classes of codes have been computed, of which more than 800 000 are optimal codes. Nearly 200 000 generator matrices can be found on the attached compact disc, of which more than 70 000 generate optimal codes. The complete set of computed generator matrices can be downloaded from the web-site mentioned above. These codes are all pairwise inequivalent. More precisely, they are representatives of different semilinear isometry classes.

On the side of the reader we assume only a basic knowledge of Linear Algebra and Algebra. Many fundamental notions are reviewed in the text. Readers with a background in field theory may skip Chapter 3. We should also mention what this book for one reason or the other does not cover. For instance, we do not discuss algebraic geometric codes, in particular the generalized version of Goppa-codes. Also not included are convolutional codes, Turbo codes, LDPC codes, codes over rings, e.g. $\mathbb{Z}_4$, and decoding methods using Tanner-graphs. All this, as well as the connection between codes and designs and a deeper account on the theory of self-dual codes had to be left out. To this end, we refer the interested reader to the excellent literature on these topics, for instance the recent books by Pless and Huffman [94], Moon [153], Nebe, Rains and Sloane [157]. The "classic" for nearly 30 years, the book by MacWilliams and Sloane [139] from 1977 is still astonishingly comprehensive. The connections between codes and designs are described in the book by Assmus and Key [5]. The Handbook of Coding Theory [163], edited by Pless and Huffman, has articles on many of these topics written by experts in the field.

The authors wish to express their sincerest thanks in particular to Karl-Heinz Zimmermann, coauthor of the German precursor book "Codierungstheorie". We also thank our colleague Reinhard Laue, to whom we owe great thanks for many stimulating discussions on the constructive theory of finite structures using group actions. Thanks are also due, of course, to our students and to the scientific community, in particular to Andries Brouwer, who maintains a very helpful table on parameters of optimal linear codes, as well as to the editors of the important two volumes of the Handbook of Coding Theory, Vera S. Pless and W. Cary Huffman. Furthermore, we greatly appreciate receiving helpful comments and suggestions from Georg Wolfgang Desch, Evi Haberberger, Oscar Jenkins, Steve Linton, Rebecca Lynn, Eric Moorhouse, Eammon O'Brien, Tim Penttila, Jens Schwaiger, Ákos Seress, Justyna Sikorska and Johannes Zwanzger.

We acknowledge financial support by the *Deutsche Forschungsgemeinschaft* and the *Österreichischer Fonds zur Förderung der wissenschaftlichen Forschung* for

helpful financial support of several research projects on these topics. These projects contributed very much to the development of the theory and to the implementation of corresponding software, as well as to the collection of data which are now available for the interested reader via email, Internet and the attached compact disc.

Last but not least, we should like to thank Ruth Allewelt, Martin Peters and Thomas Wurm from the Springer publishing company for their patient and diligent handling of this book project.

Fort Collins, Munich, Graz, Bayreuth
July 4, 2006

Anton Betten
Michael Braun
Harald Fripertinger
Adalbert Kerber
Axel Kohnert
Alfred Wassermann