Algorithms and Computation in Mathematics • Volume 17

Gabriele Nebe
Eric M. Rains
Neil J.A. Sloane

Self-Dual Codes and Invariant Theory

With 10 Figures and 34 Tables

Springer

Authors

Gabriele Nebe
Lehrstuhl D für Mathematik
Rheinisch-Westfälische
Technische Hochschule Aachen
Templergraben 64
52062 Aachen
Germany
e-mail: nebe@math.rwth-aachen.de

Neil J.A. Sloane
Internet and Network Systems Research
AT&T Shannon Labs
180 Park Avenue
Florham Park, NJ 07932-0971
USA
e-mail: njas@research.att.com

Eric M. Rains
Department of Mathematics
University of California at Davis
1 Shields Ave
Davis, CA 95616
USA
e-mail: rains@math.ucdavis.edu

Library of Congress Control Number: 2005937507

Mathematics Subject Classification (2000): 94B05, 94B60, 13A50, 16P10, 20G05; 15A66, 16D90, 68Q99, 81R99

ISSN 1431-1550

ISBN-10 3-540-30729-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30729-7 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media
springer.com
© Springer-Verlag Berlin Heidelberg 2006
Printed in The Netherlands

Typesetting: by the authors and TechBooks using a Springer LaTeX macro package
Cover design: *design & production* GmbH, Heidelberg

Printed on acid-free paper SPIN: 11587170 17/TechBooks 5 4 3 2 1 0

Preface

This book has two goals. On the one hand it develops a completely new unifying theory of self-dual codes that enables us to prove a far-reaching generalization of Gleason's theorem on weight enumerators of self-dual codes. On the other hand it is an encyclopedia that gives a very extensive list of "Types" of self-dual codes and their properties—the associated Clifford-Weil groups and their invariants, in particular. For the most important Types we give bounds on their minimal distance and updated tables of the best codes.

One of the most remarkable theorems in coding theory is Gleason's 1970 theorem [191] that the weight enumerator of a binary doubly-even self-dual code is an element of the polynomial ring generated by the weight enumerators of the Hamming code of length 8 and the Golay code of length 24. In the past thirty-five years a number of different proofs of this theorem have been given, as well as many generalizations that apply to other families of self-dual codes (see for example [34], [359], [361], [383], [454], [500]). One reason for the interest in self-dual codes is that they include some of the nicest and best-known error-correcting codes, and there are strong connections with other areas of combinatorics, group theory and (as we will mention in a moment) lattices. Self-dual codes are also of considerable practical importance, although that is outside the scope of this book.

In the past, analogues of Gleason's theorem have been derived for each new family of codes on a case-by-case basis. One of the main goals of this book is to present a generalization of Gleason's theorem that applies simultaneously to weight enumerators of self-dual codes over many different alphabets. The codes we consider are linear, which for us means that the alphabet is a module V over a ring R, and a code of length N is an R-submodule of V^N. Our theorem applies to any alphabet that is a finite module over a *quasi-chain ring*—a quasi-chain ring is a product of matrix rings over chain rings, and a *chain ring* is a ring in which the left ideals are linearly ordered by inclusion. Quasi-chain rings include finite fields, the integers mod m (e.g. $\mathbb{Z}/4\mathbb{Z}$), and more generally any finite Galois ring, as well as finite quotient rings of maximal orders in quaternion algebras. It would be incorrect to say that our theory applies to self-dual codes over *any* finite ring or module, but it certainly applies to any in which the reader is likely to be interested for the foreseeable future.[1]

The weight enumerator of a classical binary code C is a homogeneous polynomial that gives the number of codewords in C of each Hamming weight. For binary doubly-even self-dual codes this polynomial belongs to the invariant ring of a certain complex matrix group of order 192, and the fact that this ring has a very simple structure leads to Gleason's theorem: the ring is a polynomial ring with two generators, and as generators one can take the weight enumerators of the Hamming and Golay codes.

Our approach provides a general setting for this connection between self-dual codes and invariant theory. To a self-dual code C over an alphabet of size v we associate a polynomial $p_C \in \mathbb{C}[x_1, \ldots, x_v]$, the "complete weight enumerator" of C. Properties of C translate into invariance properties of p_C. For example, if the length of C is even, p_C must be invariant under the transformation $x_i \mapsto -x_i$ $(i = 1, \ldots, v)$. The polynomials with the given invariance properties then belong to a finitely generated graded ring. This makes it much easier to determine the possible p_C, and may allow one to deduce new properties of the codes, for instance to give bounds on the minimal distance.

We will define a general notion of Type of a self-dual code. Attached to each Type ρ is a finite complex matrix group $\mathcal{C}(\rho)$, the associated "Clifford-Weil group", and our main theorem (Theorem 5.5.7 and Corollary 5.7.5) shows that the invariant ring of $\mathcal{C}(\rho)$ is generated by the weight enumerators p_C of codes C of Type ρ. On the one hand this provides information about the possible codes of this Type (divisibility criteria for the length, bounds on the minimal distance, etc.), and on the other hand it makes it easier to compute the invariant ring of $\mathcal{C}(\rho)$. In fact our original investigations in [383] began as an attempt to generalize Sidelnikov's theorem [490], [491], [492], [493] that, for $m \geq 3$, the lowest degree harmonic invariant of the group $\mathcal{C}_m$ has degree 8. Since the invariant ring of $\mathcal{C}_m$ is spanned by the genus-m weight-enumerators of self-dual binary codes, this observation is reflected in the fact that 8 is the first length where there are two inequivalent Type I codes, i_2^4 and the Hamming code e_8 (see Chapter 6).

Our theory also applies to higher-order weight enumerators (sometimes called multiple or higher-genus weight enumerators), which consider m-tuples of codewords rather than single codewords. This leads to the higher-genus Clifford-Weil groups $\mathcal{C}_m(\rho) \leq GL_{v^m}(\mathbb{C})$. For $m = 1, 2, \ldots$ these groups form an infinite series for which the sequence of Molien series converges monotonically to the generating function $\sum_{N \geq 0} a_N t^N$ for the numbers a_N of equivalence classes of codes of Type ρ and length N (Cor. 5.7.7, Cor. 6.2.4). Note that this

[1] As an example, self-dual codes over the ring $\begin{pmatrix} \mathbb{Z}/4\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \\ 2\mathbb{Z}/4\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \end{pmatrix}$ are not covered by Theorem 5.5.7. Nor are codes over the group ring $\mathbb{F}_3 S_3$, where S_3 is the symmetric group of order 6.

leads to a surjection $\mathrm{Inv}(\mathcal{C}_m(\rho)) \longrightarrow \mathrm{Inv}(\mathcal{C}_{m-1}(\rho))$, analogous to the famous Siegel Φ-operator in the theory of Siegel modular forms (cf. Freitag [176]), which is presumably worth investigating further (see [381] for some initial investigations along these lines).

The Clifford-Weil groups are often very nice groups. In the case of genus-m weight enumerators (for $m \geq 1$) of self-dual binary codes, $\mathcal{C}_m(\rho)$ is the real Clifford group $\mathcal{C}_m$ of our earlier paper [383]. For the Type ρ of doubly-even self-dual binary codes, $\mathcal{C}_m(\rho)$ is the complex Clifford group $\mathcal{X}_m$ of [383]. The case $m = 1$ gives the original Gleason theorem (except for the specific identification of codes that generate the ring). In [383] we followed Bolt, Room and Wall [57], [58], [59], [536] in calling these "Clifford" groups. For self-dual codes over $\mathbb{F}_p$ containing the all-ones vector (where p is an odd prime), $\mathcal{C}_m(\rho)$ is the group $\mathcal{C}_m^{(p)}$ of [383, §7]. This is a metaplectic group, as in Weil [546], and explains why we call these "Clifford-Weil" groups in general.

These Clifford-Weil groups are also Jordan subgroups of classical Lie groups (as discussed in Alekseevskii [3], Gross and Nebe [206], Kostrikin and Tiep [334]), and provide an infinite family of examples of maximal finite matrix groups that are closely related to generalized Barnes-Wall lattices.

Besides Gleason's theorem, another remarkable fact in the background to this book is the close relationship between codes and lattices. There are some astonishing parallels between the two theories, as shown in the following list. To each of the following concepts from coding theory there is an analogue from lattice theory:

code	lattice
self-dual code	unimodular lattice
doubly-even self-dual code	even unimodular lattice
weight enumerator	theta series
invariant polynomial	modular form
MacWilliams identity	Jacobi identity
Gleason's theorem	Hecke's theorem
Molien's theorem	Selberg trace formula
Hamming code e_8	root lattice E_8
Golay code g_{24}	Leech lattice Λ_{24}

Items in the left column can be related to those in the right column by "Construction A", or one of its variants [133]. These parallels have been discussed in various articles ([500], [501], [503], Broué and Enguehard [82], [83], and most recently by Elkies [168]). One of the goals in this book, not fully realized, was to extend our main theorem to include lattices, and so to throw some additional light on the connections between codes and lattices. We were only partially successful, but the theory, presented in Chapter 9, has nevertheless led to a number of new results.

As well as lattices, another topic that has a lot in common with self-dual codes is that of quantum error-correcting codes. In fact, the construction of quantum codes was one of the initial reasons for our interest in the Clifford-Weil group. Although our main theorem does not directly apply to these codes, there are many connections to the rest of the book, and they are discussed in the final chapter.

In order to define the Type of a code in sufficient generality, we found it necessary to extend the notion of "form ring" from unitary K-theory (cf. Hahn and O'Meara [226]). In that theory, form rings are not closed under taking quotients, but with our definition, given in Chapter 1, they are. It may be worth investigating this extended notion from a K-theoretical perspective.

A note about finiteness. Although coding theory usually deals with finite alphabets (which in this book mean finite modules over finite rings), a large part of our theory is valid for arbitrary rings. In particular, the theory of form rings applies also to infinite rings. Our particular construction of the Clifford-Weil groups in Chapter 5, however, relies heavily on the finiteness of the R-module V. Consequently the proofs of the main theorems are valid only for finite form rings. On the other hand, the construction of the hyperbolic co-unitary groups applies to arbitrary form rings. We make use of this in particular in Chapter 9, where we see that the hyperbolic co-unitary groups for matrix rings over the integers coincide with Siegel modular groups.

Although this is not a textbook, our treatment is self-contained, and we have defined most of the concepts that we use, both from coding theory and invariant theory. These definitions have been kept short and expressed in our new language of form rings. As a result the book should be accessible to mathematicians, engineers and computer scientists.

The following is a brief description of the individual chapters, with emphasis on what is new. The reader is referred to the introductions to the chapters and to the table of contents for a more detailed list of what is in each chapter.

The introduction to Chapter 1 discusses how the notion of a self-dual code has been enlarged over the years. A major stimulus was the discovery in the early 1990's by Hammons, Kumar, Calderbank, Sloane and Solé [175], [91], [227] that certain notorious nonlinear binary codes could best be understood as arising from linear codes over the Galois ring $\mathbb{Z}/4\mathbb{Z}$. Our new notion of Type is defined in §1.8, after the necessary algebraic machinery has been developed in the earlier sections. In brief, a Type is a representation ρ of a form ring.

Chapter 2 begins by defining various weight enumerators associated with a code, and then follows a long section (§2.3) in which we describe all the families of self-dual codes that have been studied up to the present time as Types, using our new language of form rings. We also introduce (in §2.3.6) many new Types that treat self-dual codes over general Galois rings. Although the latter codes have so far received little attention, this may change, and in any case this section illustrates how our methods could be applied in the future if further classes of self-dual codes arise. A second long section (§2.4) then gives examples of codes and their weight enumerators for the major Types.

Chapter 2 contains two tables, Tables 2.1 (p. 78) and 2.2 (p. 79), which provide a useful list of the principal Types and the sections where they appear in the book. Another useful table appears in Chapter 11: Table 11.1 (p. 325) gives bounds on the minimal distance (used to define "extremal" codes) for the principal Types, as well as numbers ν and c such that the length must be a multiple of ν and the weights must be divisible by c. The latter property is related to the Gleason-Pierce theorem, discussed in the final section (§2.5) of Chapter 2.

Our primary interest in the book is in self-dual codes, satisfying $C^{\perp} = C$. Of course this implies that $C^{\perp\perp} = C$. Codes with this latter property are called *closed*. In Chapter 3 we attempt to identify just which families of codes are closed. Our main conclusion, which may be new, is that codes in certain finite representations of twisted rings are closed (see §3.3). In particular, the definition of Type given in Chapter 1 is strong enough to guarantee that all codes in a representation of a form ring are closed. Conversely, Theorem 3.2.8 shows that, while the notion of twisted rings may not be the only way to force codes to be closed, it is the only *natural* way. Our analysis in this chapter may be regarded as a continuation of the work of Wood [552], [553], [554], who concluded that quasi-Frobenius rings are the most general setting in which it makes sense to study codes over rings. Our analysis shows that one can work with the larger family of codes over twisted rings. The extra generality comes about because we consider bilinear forms taking values in a module rather than in a ring.

Chapter 4 examines the objects introduced in Chapter 1 from the point of view of category theory, and develops machinery that will be needed to prove the main theorems in the following chapter. The mathematical techniques used in this chapter are probably the most abstract in the book, and will be the least familiar to coding theorists. The Witt group of representations of a form ring, introduced in §4.6, will play an important role in several later chapters. A more detailed summary can be found in the introduction to this chapter. These results may also be of independent interest to people working in unitary K-theory.

Chapter 5 introduces the Clifford-Weil groups and their invariants. Table 5.1 on page 142 summarizes the principal Clifford-Weil groups and their structure. The main results of this book, Theorems 5.5.5 and 5.5.7, will be found in §5.5. They show that, under quite general conditions, the invariant ring of the Clifford-Weil group associated with a finite representation ρ of a form ring is spanned by the complete weight enumerators of self-dual isotropic codes of Type ρ (and arbitrary length). Although a simplified version was given in our announcement in [385], this is the first time that the complete statement of our main theorems have appeared in print. One of our two main theorems, Theorem 5.5.7 (p. 152), establishes this for self-dual codes defined over quasi-chain rings. The other main theorem, Theorem 5.5.5 (p. 150), establishes a similar result when the Type is a representation of a finite triangular form ring (defined in §1.9).

In fact we conjecture that a still more powerful theorem should hold, which would include both of the two main theorems as special cases. We state this "Weight Enumerator Conjecture" in two forms, Conjectures 5.5.2 and 5.7.2. An additional piece of evidence for this conjecture is provided by Theorem 5.5.3: an isotropic self-dual code of Type ρ and length N exists if and only if $\mathcal{C}(\rho)$ has an invariant of degree N.

Chapter 6 summarizes some of the results of our earlier paper [383] and relates them to the new situation. We can now give simpler proofs for some of the theorems in [383], including of course the main theorems, which are now special cases of the theorems in Chapter 5. The chief subjects of [383] were the real Clifford group $\mathcal{C}_m$ arising from genus-m weight enumerators of binary self-dual codes, and the complex Clifford group $\mathcal{X}_m$ arising in a similar way from doubly-even binary self-dual codes. The opening section of Chapter 6 gives some background information about the history of these groups, and the earlier work of several authors including—in roughly historical order—Barnes, Bolt, Room, Wall, Duke, Runge, Oura, Sidelnikov, Calderbank, Kantor, and Shor. This historical section concludes with the story of the amazing coincidence which led to the writing of the papers [92], [95], [96], and eventually to the present book.

In Chapter 7 we continue with the Types of codes defined in Chapter 2, and construct the associated form rings, representations, Clifford-Weil groups, and their invariants and Molien series. Chapters 6 and 7 include all the classical Types of codes.

Chapter 8 treats some further Types that were not covered in the previous two chapters, including codes over Galois rings, such as $\mathbb{Z}/4\mathbb{Z}$, and codes over $\mathbb{F}_{q^2} + \mathbb{F}_{q^2}u$ where $u^2 = 0$. The most important case of the latter family is when $q = 2$—such codes were studied by Bachoc [19] and Gaborit [178] in connection with the construction of quaternionic lattices.

Self-dual codes of many of the Types we discuss have been investigated, and their invariant rings determined, by a number of authors, including Bachoc, Bannai, Betsumiya, Bonnecaze, Choie, Conway, Dougherty, Gaborit, Gulliver, Harada, Huffman, Kim, Mallows, Munemasa, Otmani, Ozeki, Pless, Solé, and many others (as well as the present authors). However, this is the first time that these codes and their invariant rings have all been derived in a uniform way. Many of the results in Chapters 6–8 are new.

Chapter 9 presents our attempt to fit self-dual lattices into our framework of Types. The reader is referred to the long introductory section of that chapter for more information about its contents.

In Chapter 10 we apply our theory to study weight enumerators of maximally isotropic codes—that is, codes which, while not self-dual, are maximal subject to being isotropic. Note that, by definition, isotropic codes are also self-orthogonal. The weight enumerators of maximally self-orthogonal codes were first studied from this point of view by Mallows, Pless and Sloane [364], [366]. Our systematic approach enables us to correct some errors and omissions in the earlier work and to extend it to other families of codes. In particular, we describe the space of weight enumerators of maximal isotropic codes from the following families:

- doubly-even binary codes (Theorem 10.2.1)
- singly-even binary codes (Theorem 10.3.1)
- ternary codes (Theorem 10.4.1)
- ternary codes with **1** in the dual (Theorems 10.4.2 and 10.4.2)
- even additive trace-Hermitian self-orthogonal codes over $\mathbb{F}_4$ (Theorem 10.5.1)
- doubly-even codes over $\mathbb{Z}/4\mathbb{Z}$ (Theorem 10.6.1)

Almost all these results are new. In the second half of the chapter we use the results in Chapter 9 and the first half of the chapter to describe the space of modular forms spanned by the theta series of

- maximal even lattices of determinant 3^k (Corollary 10.7.7)
- maximal even lattices of determinant 2^k (Theorem 10.7.14)

Again we believe that these results are new.

One of the motivations for calculating these invariant rings is that it may then be possible to apply the linear programming method to obtain bounds on the minimal distance. The general "linear programming bound" for isotropic codes is the subject of §11.1.1 of Chapter 11. Section 11.1 summarizes the best upper bounds on codes of the principal Types that have been obtained by the linear programming and other methods; §11.2 then gives lower bounds.

We follow [454] in using the term *extremal* to indicate a code which has the highest minimal distance permitted by the appropriate linear programming bound, and *optimal* to indicate a code which has the actual highest minimal distance of any code of the given Type and length (an extremal code is automatically optimal, but in general no extremal code may exist). Table 11.1 (p. 325) summarizes what extremal means for the principal Types. The final section, §11.3, gives a summary of what is presently known about the existence of extremal and optimal codes of modest lengths. These are based on earlier tables in [454] and other sources. Although most of the material in this chapter is not new, it has not been collected in one place before. (See also the survey article of Huffman [282].)

In Chapter 12 we discuss what is presently known about the enumeration of self-dual codes of the main Types. Again this is an update of earlier tables. The main tool for these enumerations are the mass formulae given in §12.1.

The final chapter, Chapter 13, gives a brief discussion of quantum codes and their constructions and bounds. The last section, §13.6 gives a table of the best additive $[[N,k,d]]$ binary codes presently known. This is an updated version of the table in Calderbank, Rains, Shor and Sloane [96]. Again we refer the reader to the introduction to this chapter for a more detailed description of its contents and its relationship to the rest of the book.

The book concludes with an extensive bibliography. This seemed desirable, since few readers will be familiar with all the topics we mention. Furthermore, there are a large number of papers on self-dual codes, which have been scattered throughout the literature on engineering, mathematics and computer science. Besides these conventional references, we have also given cross-references to the *On-Line Encyclopedia of Integer Sequences* [504] for various number sequences that occur (coefficients of Molien series, minimal distances of optimal codes of various Types, etc.). For an example, see the reference to sequence A001399 in Eq. (5.8.1) on page 169.

A summary of some of the new results appeared in [385].

In this book we will mostly only discuss *self-dual* codes. Two topics that we will not treat are *isodual* codes, that is, codes which are equivalent to their duals under an appropriate notion of equivalence (cf. Conway and Sloane [132]), and *formally self-dual* codes, that is, possibly nonlinear codes which the property that their weight enumerator coincides with its MacWilliams transform (cf. Betsumiya, Gulliver and Harada [40], Betsumiya and Harada [44], [43], and Gulliver and Harada [210]). An isodual code is automatically formally self-dual. However, we do give a definition of formally self-dual in the language of Types at the end of §5.7.

We will also not say anything about *decoding* self-dual codes. Most of the existing work on this subject is concerned with classical codes such as the Golay and extended quadratic residue codes; little has been done on decoding self-dual codes over rings, except for the octacode of §2.4.9 (or its *alter ego* the Nordstrom-Robinson code). Readers interested in decoding are referred to the following papers: Amrani and Beéry [4], Amrani, Beéry and Vardy [5], Amrani, Beéry, Vardy, Sun and van Tilborg [6], Anderson [8], Blaum and Bruck [53], Bossert [69], Conway and Sloane [126], Dodunekov, Zinoviev and Nilsson [145], Esmaeili, Gulliver and Khandani [169], Fekri, McLaughlin, Mersereau and Schafer [171], Gaborit, Kim and Pless [184], Gordon [196], Greferath and Vellbinger [202] Greferath and Viterbo [203] Hammons, Kumar, Calderbank, Sloane and Solé [227], Higgs and Humphreys [264], Kim, Mellinger and Pless [305], Kim and Pless [306], Ping and Yeung [407], Pless [418], [421], Reed, Yin and Truong [456], Rifà [459], Solomon [509], Vardy [532], Wolfmann [549], [550], Yuan and Leung [564].

Acknowledgements

Much of this work was carried out while E.M.R. and N.J.A.S. were together at AT&T Shannon Labs. We thank AT&T Shannon Labs for making it possible for G.N. to visit the Labs in 1999 and 2002. Part of the work was done during G.N.'s visit to Harvard University with a Radcliffe Fellowship. G.N. thanks the Radcliffe Institute for its kind invitation. Since 2004, E.M.R. has been supported in part by NSF Grant DMS-0401387. Many of the calculations involving matrix groups and their Molien series and invariants were carried out with the computer algebra system MAGMA [68], [100].

We would like to thank Matthias Künzer, who made valuable comments during the course G.N. gave on the topics of this book in the summer of 2005 at RWTH Aachen. We also thank Koichi Betsumiya, Young-Ju Choie, Philippe Gaborit, Masaaki Harada, Akihiro Munemasa, Patric Östergård, Vera Pless, Heinz-Georg Quebbemann, Patrick Solé and John van Rees for providing helpful comments on the manuscript.

Although we have made every effort to be careful, it is inevitable that there will be errors in a book of this size, for which we apologize in advance. We would appreciate hearing of any corrections, as well as updates to the tables. Such items will be added to the web site for the book, which is www.research.att.com/∼njas/doc/cliff2.html. They may be sent to any of the authors. Our email addresses are nebe@math.rwth-aachen.de, rains@math.ucdavis.edu and njas@research.att.com.

Aachen, Davis and Florham Park
October, 2005

Gabriele Nebe ·
Eric M. Rains · N. J. A. Sloane

General notation

Unless specified otherwise a ring (usually denoted by R) has an identity element $1 \neq 0$ and may be finite or infinite, commutative or noncommutative. Rings are always associative. Codewords are generally viewed as row vectors and the alphabet is a left R-module. The following table lists symbols that are used throughout the book.

List of Symbols.

Symbol	*Meaning*	*See*
$A\,.\,B$	group with normal subgroup isomorphic to A and quotient isomorphic to B	
$A \rtimes B$	split extension or semidirect product	
$A \wr B$	wreath product	
$A\,\mathsf{Y}B$	central product	
$\mathrm{Aut}(\rho)$	automorphism group	Defn 1.11.1
$C \leq V$	the code C is a submodule of V	Defn 1.2.1
$C^{\perp}$	dual code	Defn 1.2.1
$C \otimes R$	code C promoted to a larger ring	Rem. 2.1.10
$\mathbb{C}$	complex numbers	
$\mathcal{C}(\rho)$	Clifford-Weil group	Defn 5.3.1
$\mathcal{C}_m(\rho)$	Clifford-Weil group of genus m	Defn 5.3.4
$\mathcal{C}_m$	real Clifford group of genus m	§6.2
$\mathcal{C}_m^{(p)}$	p-Clifford group of genus m	§6.2
cwe	complete weight enumerator	Defn 2.1.2
cwe_m	genus-m complete weight enumerator	Defn 2.1.7
$e(\tau)$	$\exp(2\pi i \tau)$	Eq. (9.1.1)
$\mathrm{Ev}_n(S)$	even matrices	Defn 1.10.4
$\mathbb{F}_q$	field of order q	
fwe	full weight enumerator	Defn 2.1.3
$\widehat{G}$	character group	Defn 2.2.1
$\mathrm{GL}_n(\mathbb{F}_q)$	general linear group	
$H^{\#}$	dual subgroup	Defn 2.2.1
$\mathbb{H}$	real quaternions	
$H_{\iota,u_\iota,v_\iota}$	MacWilliams transform in $\mathfrak{U}(R,\varPhi)$	Eq. (5.2.23)
$h_{\iota,u_\iota,v_\iota}$	MacWilliams transform in $\mathcal{C}(\rho)$	Eq. (5.3.1)
hwe	Hamming weight enumerator	Defn 2.1.2

Symbol	*Meaning*	*See*
I or I_n	$n \times n$ unit matrix	
$I \trianglelefteq R$	I is an ideal in R	
Inv	invariant ring	Eq. (5.6.3)
$\mathrm{Inv}(G, S)$	relative invariants	Defn 5.6.5
$\mathrm{Mat}_m(R)$	$m \times m$ matrices over R	
$\mathrm{Mat}_{m \times n}(R)$	$m \times n$ matrices over R	
MS	Molien series	Eq. (5.6.1)
$O_n(\mathbb{F}_q)$	orthogonal group	
$P(R, \varPhi)$	parabolic subgroup of $\mathfrak{U}(R, \varPhi)$	Defn 5.1.1
$P(\rho)$	parabolic subgroup of $\mathcal{C}(\rho)$	Defn 5.1.2
$\mathbb{Q}$	rational numbers	
$\mathbb{R}$	real numbers	
$(R, M, \psi, \varPhi)$	form ring	Defn 1.7.1
$\rho, (V, \rho_M, \rho_\varPhi, \beta)$	representation of form ring	Defn 1.7.2
$\mathrm{Sp}_{2n}(\mathbb{F}_q)$	symplectic group	
S_N	symmetric group of order $N!$	
swe^ρ	symmetrized weight enumerator	Defn 2.1.5
swe^ρ_m	genus-m symmetrized weight enumerator	Defn 2.1.8
tr	transposed matrix	
tr, Tr	trace operators	
$T(M)$	triangular twisted ring	Defn 1.5.1
$T(M, \varPhi)$	triangular form ring	§1.9
$U_n(\mathbb{F}_{q^2})$	unitary group	
$\mathfrak{U}(R, \varPhi)$	hyperbolic co-unitary group	Defn 5.2.4
$\mathfrak{U}_m(R, \varPhi)$	hyperbolic co-unitary group of genus m	Defn 5.2.8
V^*	dual in sense of linear algebra, space of linear functionals	
$\mathrm{WAut}(\rho)$	weak automorphism group	Defn 1.11.2
$\mathcal{X}_m$	complex Clifford group of genus m	§6.2
Z_n	cyclic group of order n	
$\mathbb{Z}_n$	n-adic integers	
$\mathbb{Z}/n\mathbb{Z}$	ring of integers mod n	
$\mathbf{1}$	all-ones vector	Ex. 1.8.4
$\{\!\{\ \}\!\}, \lambda$	structure maps	Defn 1.6.1, 4.1.1

Contents

List of Tables

List of Figures

1

The Type of a Self-Dual Code

To motivate these initial definitions, we begin by remarking that in the classical theory (cf. van Lint [350], MacWilliams and Sloane [361], Pless, Huffman and Brualdi [427], Rains and Sloane [454]) a linear error-correcting code C is a subspace of a vector space V over a finite field $\mathbb{F}$, with inner products of codewords taking values in $\mathbb{F}$ itself. The classical theory was enlarged in the early 1990's by the discovery by Hammons, Kumar, Calderbank, Sloane and Solé [175], [91], [227] that certain notorious *nonlinear* binary codes (the Nordstrom-Robinson, Kerdock and Preparata codes) could best be understood as arising from *linear* codes over the ring $\mathbb{Z}/4\mathbb{Z}$, and, in the case of the Kerdock code, from a self-dual linear code over $\mathbb{Z}/4\mathbb{Z}$.

A few years later, an important application of coding theory to quantum computers required the use of additive (but nonlinear) codes over $\mathbb{F}_4$ (Calderbank, Rains, Shor and Sloane [95], [96] and Chapter 13 below).

Furthermore, codes over rings such as $\mathbb{Z}/8\mathbb{Z}$ arise naturally in studying "Phase Shift Keying" or PSK modulation schemes—see for example Anderson [7, §3.4], Piret [408].

Thus it became clear that the theory should consider codes over rings as well as over fields, and that weaker notions of linearity should be permitted.

Concerning the weights of codewords in a self-dual code, it is easy to show that in a self-dual code over $\mathbb{F}_2$ the weight of every codeword must be even, in a self-dual code over $\mathbb{F}_3$ the weight of every codeword is a multiple of 3, and in a Hermitian self-dual code over $\mathbb{F}_4$ the weight of every codeword is even. Furthermore, there are many well-known self-dual codes over $\mathbb{F}_2$ whose weights are divisible by 4. Since these four families were the self-dual codes of main interest in the classical theory, they were called codes of *Types* I, III, IV and II respectively. In fact, as we will discuss in §2.5, a theorem of Gleason and Pierce shows that these are essentially the only possible divisibility restrictions that can be placed on the weights of self-dual codes over finite fields.

But once one allows self-dual codes to be defined over rings, there are other possible constraints that can be placed on the weights, and so in [454] we defined nine different Types of self-dual codes, each with its own separate definition.

One of the goals of this book is to introduce a more formal notion of the Type of a self-dual code, which will allow us to give a unified treatment of all the earlier definitions as well as a number of new ones. The new framework is also broad enough to include both unimodular and even–unimodular lattices, as we shall see in Chapter 9.[1]

In this framework, the *symbols* in the codewords belong to a left R-module V (the *alphabet*) where R is a ring, assumed to contain a unit 1, but which may be commutative or noncommutative, finite or infinite. A *code* C of *length* N will be an R-submodule of V^N for some positive integer N. A *codeword* $c \in C$ is an element of V^N and R is the *ground ring* underlying the code, in the sense that if $c \in C$ and $r \in R$ then $rc \in C$.

In the classical theory, inner products of codewords take values in the ground ring (which is usually the field of symbols, or a subfield if a trace is used to define the inner product). Now we allow the additional freedom that inner products of codewords will be defined by *bilinear forms* taking values in some abelian group A. For finite rings R, this abelian group A is usually a subgroup of $\mathbb{Q}/\mathbb{Z}$. This makes it possible to describe the MacWilliams transformation with respect to the $\mathbb{Q}/\mathbb{Z}$-valued bilinear forms as a complex linear transformation.

To specify additional properties of these codes, such as restrictions on the weights of codewords, or that the code contains the all-ones vector, we will use *quadratic maps* taking values in A; these are sums of quadratic forms and linear maps. We will therefore begin our discussion by defining quadratic maps in §1.1. In §1.2 we give the definition of a code and of the notions of *dual*, *self-orthogonal*, *self-dual* and *isotropic* code. To define a Type we will need the important concept of a *form ring*: this is defined in §1.7; §§1.3-1.6 contain technical material needed for this definition. Finally, the Type of a self-dual code is defined in §1.8. In brief, a Type is a *representation* ρ of a form ring (R, M, ψ, Φ). *Equivalences* and *automorphism groups* are defined using the language of Types in §1.11, and §1.12 defines the *shadow* of a code in this language.

1.1 Quadratic maps

Definition 1.1.1. Let V and A be abelian groups (see the preceding paragraphs for motivation). An *A-valued bilinear form on V* is a $\mathbb{Z}$-module homomorphism

$$\beta : V \otimes_{\mathbb{Z}} V \to A \,.$$

[1] Although so far "modular" lattices (Quebbemann [439]) do not fit into this framework.

If V is a left R-module for some ring R, then the set of all A-valued bilinear forms on V is a right $(R \otimes R)$-module, where the action is defined by

$$\beta(r \otimes s)(x, y) := \beta(rx, sy) \text{ for all } x, y \in V \text{ and all } r, s \in R\,.$$

This $(R \otimes R)$-module is denoted by $\mathrm{Bil}(V, A) = \mathrm{Bil}_{\mathbb{Z}}(V, A)$. An *$A$-valued quadratic map on V* is a map $\phi : V \to A$ such that

$$\phi(x+y+z)+\phi(x)+\phi(y)+\phi(z) = \phi(x+y)+\phi(x+z)+\phi(y+z)+\phi(0); \quad (1.1.1)$$

or, equivalently, such that the map $\phi : V \times V \to A$ given by

$$\phi(x, y) := \phi(x + y) - \phi(x) - \phi(y) + \phi(0) \quad (1.1.2)$$

is $\mathbb{Z}$-bilinear. A quadratic map ϕ on V is said to be *pointed* if $\phi(0) = 0$, *even* if $\phi(-x) = \phi(x)$, and *homogeneous* if it is both pointed and even. We denote the abelian group of quadratic maps from V to A by $\mathrm{Quad}(V, A)$ and the subgroup of pointed maps by $\mathrm{Quad}_0(V, A)$.

If 2 acts invertibly on A, for example, then a quadratic map ϕ is the sum of a homogeneous quadratic map (given by $x \mapsto \frac{1}{2}(\phi(x) + \phi(-x)) - \phi(0)$), a linear map (given by $x \mapsto \frac{1}{2}(\phi(x) - \phi(-x))$) and the constant $\phi(0)$.

Lemma 1.1.2. *Let $\phi : V \to A$ be a quadratic map. For all $n \in \mathbb{Z}$ and all $x \in V$,*

$$\phi(nx) = \frac{n(n+1)}{2}\phi(x) + \frac{n(n-1)}{2}\phi(-x) + (1 - n^2)\phi(0)\,. \quad (1.1.3)$$

Proof. Applying (1.1.1) with $y = -x$, we find that

$$\phi(z + x) - 2\phi(z) + \phi(z - x) \quad (1.1.4)$$

is independent of z. By evaluating (1.1.4) at $z = 0, x, 2x, \ldots$ we obtain (1.1.3) for $n \geq 0$; evaluating (1.1.4) at $z = -x, -2x, \ldots$ we obtain (1.1.3) for $n < 0$. □

Corollary 1.1.3. *If the quadratic map $\phi : V \to A$ is homogeneous, then*

$$\phi(nx) = n^2\phi(x) \quad (1.1.5)$$

for all integers n and all $x \in V$.

In our applications, bilinear forms will arise from the requirement that two vectors in a self-dual code should have inner product zero. Some of the quadratic maps arise from specializations of bilinear forms, others when we impose constraints on the weights of codewords (cf. Example 1.2.2).

The reason we do not use condition (1.1.5) as well as (1.1.1) when defining a quadratic map is that (1.1.5) only applies to homogeneous quadratic functions, whereas our quadratic maps may also have a linear or constant part, for example when we study codes that must contain the all-ones vector (cf. Example 1.8.4). Furthermore, if the characteristic is 2, (1.1.5) is always satisfied.

Since the obvious action of the underlying ring R on quadratic maps is not linear, we introduce the notion of a "qmodule", generalizing the notion of a linear R-module.

Definition 1.1.4. Let R be a ring. A (right) *R-qmodule* is an abelian group Φ equipped with a pointed quadratic map $r \mapsto [r]$ from R to $\mathrm{End}(\Phi)$ (with $[r]$ acting on Φ on the right) such that $[1] = 1$, $[r][s] = [rs]$. A homomorphism between qmodules Φ_1 and Φ_2 is a map f such that $f(\phi_1 + \phi_2) = f(\phi_1) + f(\phi_2)$ and $f(\phi_1[r]_1) = f(\phi_1)[r]_2$ for all $\phi_1, \phi_2 \in \Phi, r \in R$.

Example 1.1.5. The group $\Phi = \mathrm{Quad}_0(V, A)$ of all pointed quadratic maps on a left R-module V is a right R-qmodule, with

$$(\phi[r])(v) := \phi(rv), \quad \text{for } r \in R, \phi \in \Phi, v \in V\,.$$

Example 1.1.6. If M is a right R-module, then $x[r] = xr$ gives M an R-qmodule structure. A qmodule obtained this way is called *linear*

Example 1.1.7. The abelian group $\mathbb{Z}/4\mathbb{Z}$ admits a natural $\mathbb{Z}/2\mathbb{Z}$-qmodule structure, given by

$$x[0] = 0, \quad x[1] = x, \text{ for } x \in \mathbb{Z}/4\mathbb{Z}\,. \tag{1.1.6}$$

1.2 Self-dual and isotropic codes

We can now define the basic coding-theoretic concepts that will be used throughout the book.

Definition 1.2.1. Let V be a left R-module, A an abelian group, $M \subset \mathrm{Bil}(V, A)$ a set of A-valued $\mathbb{Z}$-bilinear forms on V, and $\Phi \subset \mathrm{Quad}_0(V, A)$ a set of A-valued pointed quadratic maps on V. An R-submodule $C \leq V$ is called a *code*. Let $C \leq V$ be a code. The *dual* of C (with respect to M) is

$$C^{\perp} := \{v \in V \mid m(c, v) = 0, \text{ for all } m \in M, c \in C\}\,. \tag{1.2.1}$$

Generalizing the standard terminology (cf. [361], [454]), we call C *self-orthogonal* (with respect to M) if $C \subset C^{\perp}$ and *self-dual* if $C = C^{\perp}$. Furthermore, C is *isotropic* (with respect to (M, Φ)) if C is self-orthogonal with respect to M, and also $\phi(c) = 0$ for all $\phi \in \Phi$, $c \in C$. Hence:

$$\begin{gathered}\{\text{ self-orthogonal codes with respect to } M\ \} \\ \bigcup \\ \{\text{ (self-orthogonal) isotropic codes with respect to } (M,\Phi)\ \} \\ \bigcup \\ \{\text{ self-dual isotropic codes with respect to } (M,\Phi)\ \}\,.\end{gathered}$$

Note that according to this definition, our codes are always "linear": for us this means "an R-submodule of an R-module".

Remark. If $C \leq V$ is an R-submodule and $\beta \in \mathrm{Bil}(V,A)$ is such that $\beta(c,c') = 0$ for all $c,c' \in C$ (i.e. C is self-orthogonal with respect to β), then clearly $\beta(r \otimes s)(c,c') = \beta(rc, sc') = 0$ for all $r,s \in R$ and $c,c' \in C$, since C is an R-module. So when defining self-orthogonal codes we may as well assume that M is an $(R \otimes R)$-submodule of $\mathrm{Bil}(V,A)$.

Example 1.2.2. Classical doubly-even self-dual (or Type II) binary codes (self-dual codes in which the weight of every codeword is a multiple of 4) arise in this framework as follows. As usual, x_i denotes the i-th component of the vector $x = (x_1,\ldots,x_N) \in \mathbb{F}_2^N$. We take $R := \mathbb{F}_2$, $V := \mathbb{F}_2^N$, $A := \frac{1}{4}\mathbb{Z}/\mathbb{Z}$,

$$M := \{0, m_0\} \subset \mathrm{Bil}(V, \frac{1}{4}\mathbb{Z}/\mathbb{Z}), \text{ where } m_0(x,y) := \sum_{i=1}^{N} \frac{1}{2} x_i y_i\,,$$

and

$$\Phi := \{0, \phi_0, 2\phi_0, 3\phi_0\} \subset \mathrm{Quad}_0(V, \frac{1}{4}\mathbb{Z}/\mathbb{Z}) \text{ where } \phi_0(x) := \sum_{i=1}^{N} \frac{1}{4} x_i^2\,.$$

Then self-dual isotropic codes with respect to (M,Φ) are precisely the doubly-even self-dual binary codes of length N (for $m_0(u,v) = 0$ ensures that the mod-2 inner product $u \cdot v$ is zero, and $\phi_0(u) = 0$ guarantees that the weight of u is a multiple of 4).

As already mentioned, our goal is to give a general definition of the "Type" of a self-dual code. Definition 1.2.1 does not quite do this, since the triple (V,M,Φ) depends on the length of the code, whereas the notion of "Type" should not. To avoid this difficulty we introduce the notion of a representation of a form ring (§1.7). Changing the length of the code will then involve changing only the representation of the form ring by adding orthogonal summands. The appropriate setting for defining isotropic codes is the notion of a "quadratic pair" (M,Φ) over R, which will be introduced in §1.6.

1.3 Twisted modules and their representations

The $(R \otimes R)$-submodules M of $\mathrm{Bil}(V,A)$ used in the previous section have a naturally defined "twist" map τ which interchanges the arguments. More generally, we have:

Definition 1.3.1. A *twisted R-module M* is a right $(R \otimes R)$-module together with an automorphism $\tau : M \to M$ such that $\tau(m(r \otimes s)) = \tau(m)(s \otimes r)$, for all $m \in M, r \in R, s \in R$, satisfying $\tau^2 = 1$.

Example 1.3.2. If V is an R-module and A an abelian group, then $M := \mathrm{Bil}(V, A)$ is a twisted R-module, where $\tau : M \to M$ is given by $\tau(m)(x, y) := m(y, x)$.

Definition 1.3.3. A *representation* $\rho := (V, \rho_M)$ of a twisted R-module M consists of an R-module V and a twisted R-module homomorphism $\rho_M : M \to \mathrm{Bil}(V, A)$ (for some abelian group A) that is compatible with the twist τ in Example 1.3.2, i.e. which satisfies

$$\rho_M(\tau(m))(x, y) = \rho_M(m)(y, x), \quad \text{for } x, y \in V, m \in M\,. \tag{1.3.1}$$

The representation ρ is said to be *finite* if R and V are finite sets and $A = \mathbb{Q}/\mathbb{Z}$.

We generalize the notion of dual code with respect to a set of bilinear forms given in the previous section to the dual code in a representation.

Definition 1.3.4. Let $\rho = (V, \rho_M)$ be a representation of a twisted R-module M. Let $C \leq V$ be a code. The *dual of C* with respect to ρ is defined to be

$$C^{\perp} := \{v \in V \mid \rho_M(m)(c, v) = 0, \text{ for } m \in M, c \in C\}\,. \tag{1.3.2}$$

We will sometimes write $C^{\perp,\rho}$ when it is necessary to specify ρ. If $C \subset C^{\perp,\rho}$ we say that C is a *self-orthogonal code in* (*the representation*) ρ; if $C = C^{\perp,\rho}$ we say C is a *self-dual code in* (*the representation*) ρ.

1.4 Twisted rings and their representations

The case when M is *isomorphic* to R as a right R-module is especially important. One can think of this as specializing only one nonsingular bilinear form β on V and taking M to be the $1 \otimes R$-submodule of $\mathrm{Bil}(V, A)$ spanned by β. (Here we use "nonsingular" in its classical sense. For the formal definition see Definition 3.2.1 in Chapter 3.) If the code C is an R-submodule of V, we have

$$C^{\perp,\beta} = \{v \in V \mid \beta(v, c) = 0 \text{ for all } c \in C\}\,, \tag{1.4.1}$$

and for any $v \in C^{\perp,\beta}$ we have $m(v, c) = 0$ for all $m \in M$ and $c \in C$.

Definition 1.4.1. A *twisted ring* (R, M, ψ) consists of a ring R, a twisted R-module M and a right R-module isomorphism $\psi : R_R \to M_{1 \otimes R}$, such that $\epsilon := \psi^{-1}(\tau(\psi(1)))$ is a unit in R. Then ϵ is called the *associated unit* defined by the involution τ.