

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable for prosecution under the German Copyright Law.

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

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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

Contents

Preface	v
List of Symbols	xiv
List of Tables	xxv
List of Figures	xxvii
1 The Type of a Self-Dual Code	1
1.1 Quadratic maps	2
1.2 Self-dual and isotropic codes	4
1.3 Twisted modules and their representations	5
1.4 Twisted rings and their representations	6
1.5 Triangular twisted rings	9
1.6 Quadratic pairs and their representations	11
1.7 Form rings and their representations	13
1.8 The Type of a code	15
1.9 Triangular form rings	18
1.10 Matrix rings of form rings and their representations	19
1.11 Automorphism groups of codes	22
1.12 Shadows	24
2 Weight Enumerators and Important Types	29
2.1 Weight enumerators of codes	29
2.2 MacWilliams identity and generalizations	35
2.2.1 The weight enumerator of the shadow	39
2.3 Catalogue of important types	39
2.3.1 Binary codes	40
2	40
2_I	41
2_{II}	41
2_S	41
2.3.2 Euclidean codes	42
4^E	42

	q^E (even)	43
	q_{II}^E	44
	3	45
	q^E (odd)	46
	q_1^E (odd)	46
2.3.3	Hermitian codes	47
	4^H	47
	q^H	47
	q_1^H	48
2.3.4	Additive codes	48
	4^{H+}	48
	q^{H+} (even)	49
	q_1^{H+} (even)	49
	q_{II}^{H+} (even)	50
	$q_{II,1}^{H+}$ (even)	50
	q^{H+} (odd)	50
	q_1^{H+} (odd)	51
2.3.5	Codes over Galois rings $\mathbb{Z}/m\mathbb{Z}$	51
	$4^{\mathbb{Z}}$	52
	$m^{\mathbb{Z}}$	53
	$m_1^{\mathbb{Z}}$	54
	$m_{II}^{\mathbb{Z}}$	54
	$m_{II,1}^{\mathbb{Z}}$	55
	$m_S^{\mathbb{Z}}$	55
2.3.6	Codes over more general Galois rings	55
	$GR(p^e, f)^E$	55
	$GR(p^e, f)_1^E$	56
	$GR(p^e, f)_{p^s}^E$	56
	$GR(2^e, f)_{2^s}^E$	57
	$GR(2^e, f)_{II}^E$	57
	$GR(2^e, f)_{II,2^s}^E$	58
	$GR(p^e, f)^H$	58
	$GR(p^e, f)_{p^s}^H$	58
	$GR(p^e, f)^{H+}$	59
	$GR(p^e, f)_{p^s}^{H+}$	59
2.3.7	Linear codes over p -adic integers	60
	\mathbb{Z}_p	60
	More general p -adic integers	60
2.4	Examples of self-dual codes	60
2.4.1	2: Binary codes	60
	2 _I : Singly-even binary self-dual codes	61
	2 _{II} : Doubly-even binary self-dual codes	61
2.4.2	4^E : Euclidean self-dual codes over \mathbb{F}_4	64
2.4.3	q^E (even or odd): Euclidean self-dual codes over \mathbb{F}_q	65

2.4.4	q_{II}^E : Generalized doubly-even self-dual codes	65
2.4.5	3: Euclidean self-dual codes over \mathbb{F}_3	67
2.4.6	4^H : Hermitian self-dual codes over \mathbb{F}_4	68
2.4.7	q^H : Hermitian self-dual linear codes over \mathbb{F}_q	68
2.4.8	4^{H+} : Trace-Hermitian additive codes over \mathbb{F}_4	69
2.4.9	4^Z : Self-dual codes over $\mathbb{Z}/4\mathbb{Z}$	70
2.4.10	Codes over other Galois rings	76
2.4.11	\mathbb{Z}_p : Codes over the p -adic numbers	77
2.5	The Gleason-Pierce Theorem	80
3	Closed Codes	83
3.1	Bilinear forms and closed codes	83
3.2	Families of closed codes	86
3.2.1	Codes over commutative rings	88
3.2.2	Codes over quasi-Frobenius rings	89
3.2.3	Algebras over a commutative ring	90
3.2.4	Direct summands	94
3.3	Representations of twisted rings and closed codes	94
3.4	Morita theory	96
3.5	New representations from old	98
3.5.1	Subquotients and quotients	98
3.5.2	Direct sums and products	99
3.5.3	Tensor products	100
4	The Category Quad	103
4.1	The category of quadratic groups	104
4.2	The internal hom-functor $\mathbb{I}Hom$	108
4.3	Properties of quadratic rings	113
4.4	Morita theory for quadratic rings	116
4.5	Morita theory for form rings	120
4.6	Witt rings, groups and modules	121
5	The Main Theorems	129
5.1	Parabolic groups	130
5.2	Hyperbolic co-unitary groups	131
5.2.1	Generators for the hyperbolic co-unitary group	136
5.3	Clifford-Weil groups	139
5.4	Scalar elements in $\mathcal{C}(\rho)$	142
5.5	Clifford-Weil groups and full weight enumerators	149
5.6	Results from invariant theory	155
5.6.1	Molien series	155
5.6.2	Relative invariants	158
5.6.3	Construction of invariants using differential operators	160
5.6.4	Invariants and designs	161
5.7	Symmetrizations	162

5.8	Example: Hermitian codes over \mathbb{F}_9	167
6	Real and Complex Clifford Groups	171
6.1	Background	171
6.2	Runge's theorems	174
6.3	The real Clifford group \mathcal{C}_m	177
6.4	The complex Clifford group \mathcal{X}_m	182
6.5	Barnes-Wall lattices	184
6.6	Maximal finiteness in real case	188
6.7	Maximal finiteness in complex case	190
6.8	Automorphism groups of weight enumerators	190
7	Classical Self-Dual Codes	193
7.1	Quasisimple form rings	193
7.2	Split type	195
7.2.1	q^{lin} : Linear codes over \mathbb{F}_q	196
	Clifford-Weil groups	198
	\mathbb{F}_2 , Genus 1	198
	\mathbb{F}_2 , Genus 2	199
7.3	Hermitian type	201
7.3.1	q^{H} : Hermitian self-dual codes over \mathbb{F}_q	202
	Clifford-Weil groups	202
	The case $q = 4$	203
	The case $q = 9$	206
7.4	Orthogonal (or Euclidean) type, p odd	207
7.4.1	q^{E} (odd): Euclidean self-dual codes over \mathbb{F}_q	207
	Clifford-Weil groups (q odd)	207
	The case $q = 3$	209
	The case $q = 3$, genus 2	210
	The case $q = 9$	211
	The case $q = 5$	212
7.5	Symplectic type, p odd	213
7.5.1	$q^{\text{H}+}$ (odd): Hermitian \mathbb{F}_r -linear codes over \mathbb{F}_q , $q = r^2$..	214
	Clifford-Weil groups (genus g)	214
	The case $q = 9$, genus 1	215
7.6	Characteristic 2, orthogonal and symplectic types	215
7.6.1	$q^{\text{H}+}$ (even): Hermitian \mathbb{F}_r -linear codes over \mathbb{F}_q , $q = r^2$..	217
	Clifford-Weil groups (genus g)	217
	The case $q = 4$, genus 1	217
	The case $q = 4$, genus 2	219
	The case $q = 16$	220
7.6.2	q^{E} (even): Euclidean self-dual \mathbb{F}_q -linear codes	220
	Clifford-Weil groups (genus g)	220
	The case $q = 2$	221
	The case $q = 4$	221

7.6.3	$q_{\text{II}}^{\text{H}+}$ (even): Even Trace-Hermitian \mathbb{F}_r -linear codes	222
	Clifford-Weil groups (genus g)	222
	The case $q = 4$, genus 1	223
7.6.4	q_{II}^{E} (even): Generalized Doubly-even codes over \mathbb{F}_q	224
	Clifford-Weil groups (genus g)	224
	The case $k = \mathbb{F}_2$, arbitrary genus	225
	The case $k = \mathbb{F}_4$, genus 1	225
	The case $k = \mathbb{F}_8$	226
8	Further Examples of Self-Dual Codes	227
8.1	$m^{\mathbb{Z}}$: Codes over $\mathbb{Z}/m\mathbb{Z}$	227
8.2	$4^{\mathbb{Z}}$: Self-dual codes over $\mathbb{Z}/4\mathbb{Z}$	230
8.2.1	$4^{\mathbb{Z}}$: Type I self-dual codes over $\mathbb{Z}/4\mathbb{Z}$	230
8.2.2	$4_{\mathbf{1}}^{\mathbb{Z}}$: Type I self-dual codes over $\mathbb{Z}/4\mathbb{Z}$ containing $\mathbf{1}$	231
8.2.3	Same, with $\mathbf{1}$ in the shadow.	233
8.2.4	$4_{\text{II}}^{\mathbb{Z}}$: Type II self-dual codes over $\mathbb{Z}/4\mathbb{Z}$	233
8.2.5	$4_{\text{II},\mathbf{1}}^{\mathbb{Z}}$: Type II self-dual codes over $\mathbb{Z}/4\mathbb{Z}$ containing $\mathbf{1}$	234
8.3	$8^{\mathbb{Z}}$: Self-dual codes over $\mathbb{Z}/8\mathbb{Z}$	234
8.4	Codes over more general Galois rings	235
8.4.1	$\text{GR}(p^e, f)^{\text{E}}$: Euclidean self-dual $\text{GR}(p^e, f)$ -linear codes.	236
8.4.2	$\text{GR}(p^e, f)^{\text{H}}$: Hermitian self-dual $\text{GR}(p^e, f)$ -linear codes.	238
8.4.3	$\text{GR}(p^e, 2l)^{\text{H}+}$: Trace-Hermitian $\text{GR}(p^e, l)$ -linear codes.	239
8.4.4	Clifford-Weil groups for $\text{GR}(4, 2)$	239
8.5	Self-dual codes over $\mathbb{F}_{q^2} + \mathbb{F}_{q^2} u$	243
9	Lattices	249
9.1	Lattices and theta series	252
9.1.1	Preliminary definitions	252
9.1.2	Modular lattices and Atkin-Lehner involutions	255
9.1.3	Shadows	260
9.1.4	Jacobi forms	261
9.1.5	Siegel theta series	261
	Jacobi-Siegel theta series and Riemann theta functions	265
	Riemann theta functions with Harmonic coefficients	268
9.1.6	Hilbert theta series	269
9.2	Positive definite form \mathbb{R} -algebras	272
9.3	Half-spaces	274
9.4	Form orders and lattices	276
9.5	Even and odd unimodular lattices	278
9.6	Gluing theory for codes	280
9.7	Gluing theory for lattices	282

10	Maximal Isotropic Codes and Lattices	285
10.1	Maximal isotropic codes	286
10.2	Maximal isotropic doubly-even binary codes	290
10.3	Maximal isotropic even binary codes	293
10.4	Maximal isotropic ternary codes	293
10.5	Maximal isotropic additive codes over \mathbb{F}_4	298
10.6	Maximal isotropic codes over $\mathbb{Z}/4\mathbb{Z}$	298
10.7	<u>Maximal even lattices</u>	<u>301</u>
10.7.1	Maximal even lattices of determinant 3^k	304
10.7.2	Maximal even and integral lattices of determinant 2^k ..	306
11	Extremal and Optimal Codes	313
11.1	Upper bounds	314
11.1.1	Extremal weight enumerators and the LP bound	314
11.1.2	Self-dual binary codes, 2_{II} and 2_I	317
11.1.3	Some other types	321
11.1.4	A new definition of extremality	324
11.1.5	Asymptotic upper bounds	326
11.2	Lower bounds	328
11.3	Tables of extremal self-dual codes	331
11.3.1	Binary codes	331
11.3.2	Type 3: Ternary codes	336
11.3.3	<u>Types 4^E and 4_{II}^E: Euclidean self-dual codes over \mathbb{F}_4</u>	<u>338</u>
11.3.4	Type 4^H : Hermitian linear self-dual codes over \mathbb{F}_4	339
11.3.5	<u>Types 4^{H+} and 4_{II}^{H+}: Trace-Hermitian codes over \mathbb{F}_4</u>	<u>340</u>
11.3.6	Type 4^Z : Self-dual codes over $\mathbb{Z}/4\mathbb{Z}$	342
11.3.7	Other types	345
12	Enumeration of Self-Dual Codes	347
12.1	The mass formulae	347
12.2	Enumeration of binary self-dual codes	350
	Interrelations between types 2_I and 2_{II}	356
12.3	Type 3: Ternary self-dual codes	360
12.3.1	Types 4^E and 4_{II}^E : Euclidean self-dual codes over \mathbb{F}_4	363
12.4	Type 4^H : Hermitian self-dual codes over \mathbb{F}_4	363
12.5	Type 4^{H+} : Trace-Hermitian additive codes over \mathbb{F}_4	365
12.6	Type 4^Z : Self-dual codes over $\mathbb{Z}/4\mathbb{Z}$	366
12.7	Other enumerations	367
13	Quantum Codes	369
13.1	Definitions	370
13.2	Additive and symplectic quantum codes	373
13.3	Hamming weight enumerators	376

13.4 Linear programming bounds	381
13.5 Other alphabets	382
13.6 A table of quantum codes	385
References	391
Index	417