J.H. Conway N.J.A. Sloane

Sphere Packings, Lattices and Groups

Third Edition

With Additional Contributions by
E. Bannai, R.E. Borcherds, J. Leech,
S.P. Norton, A.M. Odlyzko, R.A. Parker,
L. Queen and B.B. Venkov

With 112 Illustrations

Springer

J.H. Conway
Mathematics Department
Princeton University
Princeton, NJ 08540 USA
conway@math.princeton.edu

N.J.A. Sloane
Information Sciences Research
AT&T Labs – Research
180 Park Avenue
Florham Park, NJ 07932 USA
njas@research.att.com

Mathematics Subject Classification (1991): 05B40, 11H06, 20E32, 11T71, 11E12

Library of Congress Cataloging-in-Publication Data
Conway, John Horton
Sphere packings, lattices and groups. — 3rd ed. / J.H. Conway, N.J.A. Sloane.
p. cm. — (Grundlehren der mathematischen Wissenschaften ; 290)
Includes bibliographical references and index.
ISBN 978-1-4419-3134-4 ISBN 978-1-4757-6568-7 (eBook)
DOI 10.1007/978-1-4757-6568-7

1. Combinatorial packing and covering. 2. Sphere. 3. Lattice theory. 4. Finite groups. I. Sloane, N.J.A. (Neil James Alexander). 1939– . II. Title. III. Series.
QA166.7.C66 1998
511′.6—dc21 98-26950

Printed on acid-free paper.

springeronline.com

© 1999, 1998, 1993 Springer Science+Business Media New York
Originally published by Springer-Verlag New York, Inc. in 1999
Softcover reprint of the hardcover 3rd edition 1999

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, 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 of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production managed by Allan Abrams; manufacturing supervised by Thomas King.
Text prepared by the authors using TROFF.

9 8 7 6 5 4 3 2

ISBN 978-1-4419-3134-4 SPIN 10972366

Contents

Preface to First Edition v
Preface to Third Edition xv
List of Symbols lxi

Chapter 1
Sphere Packings and Kissing Numbers
J.H. Conway and N.J.A. Sloane 1

1. The Sphere Packing Problem 1
1.1 Packing Ball Bearings 1
1.2 Lattice Packings 3
1.3 Nonlattice Packings 7
1.4 n-Dimensional Packings 8
1.5 Sphere Packing Problem—Summary of Results 12
2. The Kissing Number Problem 21
2.1 The Problem of the Thirteen Spheres 21
2.2 Kissing Numbers in Other Dimensions 21
2.3 Spherical Codes 24
2.4 The Construction of Spherical Codes from Sphere Packings 26
2.5 The Construction of Spherical Codes from Binary Codes ... 26
2.6 Bounds on $A(n,\phi)$ 27
Appendix: Planetary Perturbations 29

Chapter 2
Coverings, Lattices and Quantizers
J.H. Conway and N.J.A. Sloane 31

1. The Covering Problem 31
1.1 Covering Space with Overlapping Spheres 31
1.2 The Covering Radius and the Voronoi Cells 33
1.3 Covering Problem—Summary of Results 36
1.4 Computational Difficulties in Packings and Coverings 40

2. Lattices, Quadratic Forms and Number Theory 41
2.1 The Norm of a Vector 41
2.2 Quadratic Forms Associated with a Lattice 42
2.3 Theta Series and Connections with Number Theory 44
2.4 Integral Lattices and Quadratic Forms 47
2.5 Modular Forms 50
2.6 Complex and Quaternionic Lattices 52
3. Quantizers 56
3.1 Quantization, Analog-to-Digital Conversion and Data Compression 56
3.2 The Quantizer Problem 59
3.3 Quantizer Problem—Summary of Results 59

Chapter 3
Codes, Designs and Groups
J.H. Conway and N.J.A. Sloane 63

1. The Channel Coding Problem 63
1.1 The Sampling Theorem 63
1.2 Shannon's Theorem 66
1.3 Error Probability 69
1.4 Lattice Codes for the Gaussian Channel 71
2. Error-Correcting Codes 75
2.1 The Error-Correcting Code Problem 75
2.2 Further Definitions from Coding Theory 77
2.3 Repetition, Even Weight and Other Simple Codes 79
2.4 Cyclic Codes 79
2.5 BCH and Reed-Solomon Codes 81
2.6 Justesen Codes 82
2.7 Reed-Muller Codes 83
2.8 Quadratic Residue Codes 84
2.9 Perfect Codes 85
2.10 The Pless Double Circulant Codes 86
2.11 Goppa Codes and Codes from Algebraic Curves 87
2.12 Nonlinear Codes 87
2.13 Hadamard Matrices 87
3. t-Designs, Steiner Systems and Spherical t-Designs 88
3.1 t-Designs and Steiner Systems 88
3.2 Spherical t-Designs 89
4. The Connections with Group Theory 90
4.1 The Automorphism Group of a Lattice 90
4.2 Constructing Lattices and Codes from Groups 92

Chapter 4
Certain Important Lattices and Their Properties
J.H. Conway and N.J.A. Sloane 94

1. Introduction 94
2. Reflection Groups and Root Lattices 95
3. Gluing Theory 99

4. Notation; Theta Functions 101
4.1 Jacobi Theta Functions 102
5. The n-Dimensional Cubic Lattice Z^n 106
6. The n-Dimensional Lattices A_n and A_n^* 108
6.1 The Lattice A_n 108
6.2 The Hexagonal Lattice 110
6.3 The Face-Centered Cubic Lattice 112
6.4 The Tetrahedral or Diamond Packing 113
6.5 The Hexagonal Close-Packing 113
6.6 The Dual Lattice A_n^* 115
6.7 The Body-Centered Cubic Lattice 116
7. The n-Dimensional Lattices D_n and D_n^* 117
7.1 The Lattice D_n 117
7.2 The Four-Dimensional Lattice D_4 118
7.3 The Packing D_n^+ 119
7.4 The Dual Lattice D_n^* 120
8. The Lattices E_6, E_7 and E_8 120
8.1 The 8-Dimensional Lattice E_8 120
8.2 The 7-Dimensional Lattices E_7 and E_7^* 124
8.3 The 6-Dimensional Lattices E_6 and E_6^* 125
9. The 12-Dimensional Coxeter-Todd Lattice K_{12} 127
10. The 16-Dimensional Barnes-Wall Lattice Λ_{16} 129
11. The 24-Dimensional Leech Lattice Λ_{24} 131

Chapter 5
Sphere Packing and Error-Correcting Codes
J. Leech and N.J.A. Sloane 136

1. Introduction 136
1.1 The Coordinate Array of a Point 137
2. Construction A 137
2.1 The Construction 137
2.2 Center Density 137
2.3 Kissing Numbers 138
2.4 Dimensions 3 to 6 138
2.5 Dimensions 7 and 8 138
2.6 Dimensions 9 to 12 139
2.7 Comparison of Lattice and Nonlattice Packings 140
3. Construction B 141
3.1 The Construction 141
3.2 Center Density and Kissing Numbers 141
3.3 Dimensions 8, 9 and 12 142
3.4 Dimensions 15 to 24 142
4. Packings Built Up by Layers 142
4.1 Packing by Layers 142
4.2 Dimensions 4 to 7 144
4.3 Dimensions 11 and 13 to 15 144
4.4 Density Doubling and the Leech Lattice Λ_{24} 145
4.5 Cross Sections of Λ_{24} 145
5. Other Constructions from Codes 146

5.1 A Code of Length 40 146
5.2 A Lattice Packing in $\mathbf{R}^{40}$ 147
5.3 Cross Sections of Λ_{40} 148
5.4 Packings Based on Ternary Codes 148
5.5 Packings Obtained from the Pless Codes 148
5.6 Packings Obtained from Quadratic Residue Codes 149
5.7 Density Doubling in $\mathbf{R}^{24}$ and $\mathbf{R}^{48}$ 149
6. Construction C 150
6.1 The Construction 150
6.2 Distance Between Centers 150
6.3 Center Density 150
6.4 Kissing Numbers 151
6.5 Packings Obtained from Reed-Muller Codes 151
6.6 Packings Obtained from BCH and Other Codes 152
6.7 Density of BCH Packings 153
6.8 Packings Obtained from Justesen Codes 155

Chapter 6
Laminated Lattices
J.H. Conway and N.J.A. Sloane 157

1. Introduction 157
2. The Main Results 163
3. Properties of Λ_0 to Λ_8 168
4. Dimensions 9 to 16 170
5. The Deep Holes in Λ_{16} 174
6. Dimensions 17 to 24 176
7. Dimensions 25 to 48 177
Appendix: The Best Integral Lattices Known 179

Chapter 7
Further Connections Between Codes and Lattices
N.J.A. Sloane 181

1. Introduction 181
2. Construction A 182
3. Self-Dual (or Type I) Codes and Lattices 185
4. Extremal Type I Codes and Lattices 189
5. Construction B 191
6. Type II Codes and Lattices 191
7. Extremal Type II Codes and Lattices 193
8. Constructions A and B for Complex Lattices 197
9. Self-Dual Nonbinary Codes and Complex Lattices 202
10. Extremal Nonbinary Codes and Complex Lattices 205

Chapter 8
Algebraic Constructions for Lattices
J.H. Conway and N.J.A. Sloane 206

1. Introduction 206
2. The Icosians and the Leech Lattice 207

2.1 The Icosian Group 207
2.2 The Icosian and Turyn-Type Constructions for the Leech Lattice 210
3. A General Setting for Construction A, and Quebbemann's 64-Dimensional Lattice 211
4. Lattices Over $\mathbf{Z}[e^{\pi i/4}]$, and Quebbemann's 32-Dimensional Lattice 215
5. McKay's 40-Dimensional Extremal Lattice 221
6. Repeated Differences and Craig's Lattices 222
7. Lattices from Algebraic Number Theory 224
7.1 Introduction 224
7.2 Lattices from the Trace Norm 224
7.3 Examples from Cyclotomic Fields 227
7.4 Lattices from Class Field Towers 227
7.5 Unimodular Lattices with an Automorphism of Prime Order 229
8. Constructions D and D′ 232
8.1 Construction D 232
8.2 Examples 233
8.3 Construction D′ 235
9. Construction E 236
10. Examples of Construction E 238

Chapter 9
Bounds for Codes and Sphere Packings
N.J.A. Sloane 245

1. Introduction 245
2. Zonal Spherical Functions 249
2.1 The 2-Point-Homogeneous Spaces 250
2.2 Representations of G 252
2.3 Zonal Spherical Functions 253
2.4 Positive-Definite Degenerate Kernels 256
3. The Linear Programming Bounds 257
3.1 Codes and Their Distance Distributions 257
3.2 The Linear Programming Bounds 258
3.3 Bounds for Error-Correcting Codes 260
3.4 Bounds for Constant-Weight Codes 263
3.5 Bounds for Spherical Codes and Sphere Packings 263
4. Other Bounds 265

Chapter 10
Three Lectures on Exceptional Groups
J.H. Conway 267

1. First Lecture 267
1.1 Some Exceptional Behavior of the Groups $L_n(q)$ 267
1.2 The Case $p = 3$ 269
1.3 The Case $p = 5$ 269
1.4 The Case $p = 7$ 269

1.5 The Case $p = 11$ 271
1.6 A Presentation for M_{12} 273
1.7 Janko's Group of Order 175560 273
2. Second Lecture 274
2.1 The Mathieu Group M_{24} 274
2.2 The Stabilizer of an Octad 276
2.3 The Structure of the Golay Code $\mathcal{C}_{24}$ 278
2.4 The Structure of $P(\Omega)/\mathcal{C}_{24}$ 278
2.5 The Maximal Subgroups of M_{24} 279
2.6 The Structure of $P(\Omega)$ 283
3. Third Lecture 286
3.1 The Group $Co_0 = \cdot 0$ and Some of its Subgroups 286
3.2 The Geometry of the Leech Lattice 286
3.3 The Group $\cdot 0$ and its Subgroup N 287
3.4 Subgroups of $\cdot 0$ 290
3.5 The Higman-Sims and McLaughlin Groups 292
3.6 The Group $Co_3 = \cdot 3$ 293
3.7 Involutions in $\cdot 0$ 294
3.8 Congruences for Theta Series 294
3.9 A Connection Between $\cdot 0$ and Fischer's Group Fi_{24} 295
Appendix: On the Exceptional Simple Groups 296

Chapter 11
The Golay Codes and the Mathieu Groups
J.H. Conway 299

1. Introduction 299
2. Definitions of the Hexacode 300
3. Justification of a Hexacodeword 302
4. Completing a Hexacodeword 302
5. The Golay Code $\mathcal{C}_{24}$ and the MOG 303
6. Completing Octads from 5 of their Points 305
7. The Maximal Subgroups of M_{24} 307
8. The Projective Subgroup $L_2(23)$ 308
9. The Sextet Group $2^6{:}3{\cdot}S_6$ 309
10. The Octad Group $2^4{:}\ A_8$ 311
11. The Triad Group and the Projective Plane of Order 4 314
12. The Trio Group $2^6{:}\ (S_3 \times L_2(7))$ 316
13. The Octern Group 318
14. The Mathieu Group M_{23} 319
15. The Group $M_{22}{:}2$ 319
16. The Group M_{12}, the Tetracode and the MINIMOG 320
17. Playing Cards and Other Games 323
18. Further Constructions for M_{12} 327

Chapter 12
A Characterization of the Leech Lattice
J.H. Conway 331

Chapter 13
Bounds on Kissing Numbers
A.M. Odlyzko and N.J.A. Sloane 337

1. A General Upper Bound 337
2. Numerical Results 338

Chapter 14
Uniqueness of Certain Spherical Codes
E. Bannai and N.J.A. Sloane 340

1. Introduction 340
2. Uniqueness of the Code of Size 240 in Ω_8 342
3. Uniqueness of the Code of Size 56 in Ω_7 344
4. Uniqueness of the Code of Size 196560 in Ω_{24} 345
5. Uniqueness of the Code of Size 4600 in Ω_{23} 349

Chapter 15
On the Classification of Integral Quadratic Forms
J.H. Conway and N.J.A. Sloane 352

1. Introduction 352
2. Definitions 354
2.1 Quadratic Forms 354
2.2 Forms and Lattices; Integral Equivalence 355
3. The Classification of Binary Quadratic Forms 356
3.1 Cycles of Reduced Forms 356
3.2 Definite Binary Forms 357
3.3 Indefinite Binary Forms 359
3.4 Composition of Binary Forms 364
3.5 Genera and Spinor Genera for Binary Forms 366
4. The p-Adic Numbers 366
4.1 The p-Adic Numbers 367
4.2 p-Adic Square Classes 367
4.3 An Extended Jacobi-Legendre Symbol 368
4.4 Diagonalization of Quadratic Forms 369
5. Rational Invariants of Quadratic Forms 370
5.1 Invariants and the Oddity Formula 370
5.2 Existence of Rational Forms with Prescribed Invariants 372
5.3 The Conventional Form of the Hasse-Minkowski Invariant 373
6. The Invariance and Completeness of the Rational Invariants 373
6.1 The p-Adic Invariants for Binary Forms 373
6.2 The p-Adic Invariants for n-Ary Forms 375
6.3 The Proof of Theorem 7 377
7. The Genus and its Invariants 378
7.1 p-Adic Invariants 378
7.2 The p-Adic Symbol for a Form 379

7.3 2-Adic Invariants 380
7.4 The 2-Adic Symbol 380
7.5 Equivalences Between Jordan Decompositions 381
7.6 A Canonical 2-Adic Symbol 382
7.7 Existence of Forms with Prescribed Invariants 382
7.8 A Symbol for the Genus 384
8. Classification of Forms of Small Determinant and of p-Elementary Forms 385
8.1 Forms of Small Determinant 385
8.2 p-Elementary Forms 386
9. The Spinor Genus 388
9.1 Introduction 388
9.2 The Spinor Genus 389
9.3 Identifying the Spinor Kernel 390
9.4 Naming the Spinor Operators for the Genus of f 390
9.5 Computing the Spinor Kernel from the p-Adic Symbols 391
9.6 Tractable and Irrelevant Primes 392
9.7 When is There Only One Class in the Genus? 393
10. The Classification of Positive Definite Forms 396
10.1 Minkowski Reduction 396
10.2 The Kneser Gluing Method 399
10.3 Positive Definite Forms of Determinant 2 and 3 399
11. Computational Complexity 402

Chapter 16
Enumeration of Unimodular Lattices
J.H. Conway and N.J.A. Sloane 406

1. The Niemeier Lattices and the Leech Lattice 406
2. The Mass Formulae for Lattices 408
3. Verifications of Niemeier's List 410
4. The Enumeration of Unimodular Lattices in Dimensions $n \leq 23$ 413

Chapter 17
The 24-Dimensional Odd Unimodular Lattices
R.E. Borcherds 421

Chapter 18
Even Unimodular 24-Dimensional Lattices
B.B. Venkov 429

1. Introduction 429
2. Possible Configurations of Minimal Vectors 430
3. On Lattices with Root Systems of Maximal Rank 433
4. Construction of the Niemeier Lattices 436
5. A Characterization of the Leech Lattice 439

Chapter 19
Enumeration of Extremal Self-Dual Lattices
J.H. Conway, A.M. Odlyzko and N.J.A. Sloane 441

1. Dimensions 1-16 441
2. Dimensions 17-47 441
3. Dimensions $n \geqslant 48$ 443

Chapter 20
Finding the Closest Lattice Point
J.H. Conway and N.J.A. Sloane 445

1. Introduction 445
2. The Lattices $\mathbf{Z}^n$, D_n and A_n 446
3. Decoding Unions of Cosets 448
4. "Soft Decision" Decoding for Binary Codes 449
5. Decoding Lattices Obtained from Construction A 450
6. Decoding E_8 450

Chapter 21
Voronoi Cells of Lattices and Quantization Errors
J.H. Conway and N.J.A. Sloane 451

1. Introduction 451
2. Second Moments of Polytopes 453
2.A Dirichlet's Integral 453
2.B Generalized Octahedron or Crosspolytope 454
2.C The n-Sphere 454
2.D n-Dimensional Simplices 454
2.E Regular Simplex 455
2.F Volume and Second Moment of a Polytope in Terms of its Faces 455
2.G Truncated Octahedron 456
2.H Second Moment of Regular Polytopes 456
2.I Regular Polygons 457
2.J Icosahedron and Dodecahedron 457
2.K The Exceptional 4-Dimensional Polytopes 457
3. Voronoi Cells and the Mean Squared Error of Lattice Quantizers 458
3.A The Voronoi Cell of a Root Lattice 458
3.B Voronoi Cell for A_n 461
3.C Voronoi Cell for D_n $(n \geqslant 4)$ 464
3.D Voronoi Cells for E_6, E_7, E_8 464
3.E Voronoi Cell for D_n^* 465
3.F Voronoi Cell for A_n^* 474
3.G The Walls of the Voronoi Cell 476

Chapter 22
A Bound for the Covering Radius of the Leech Lattice
S.P. Norton 478

Chapter 23
The Covering Radius of the Leech Lattice
J.H. Conway, R.A. Parker and N.J.A. Sloane 480

1. Introduction 480
2. The Coxeter-Dynkin Diagram of a Hole 482
3. Holes Whose Diagram Contains an A_n Subgraph 486
4. Holes Whose Diagram Contains a D_n Subgraph 497
5. Holes Whose Diagram Contains an E_n Subgraph 504

Chapter 24
Twenty-Three Constructions for the Leech Lattice
J.H. Conway and N.J.A. Sloane 508

1. The "Holy Constructions" 508
2. The Environs of a Deep Hole 512

Chapter 25
The Cellular Structure of the Leech Lattice
R.E. Borcherds, J.H. Conway and L. Queen 515

1. Introduction 515
2. Names for the Holes 515
3. The Volume Formula 516
4. The Enumeration of the Small Holes 521

Chapter 26
Lorentzian Forms for the Leech Lattice
J.H. Conway and N.J.A. Sloane 524

1. The Unimodular Lorentzian Lattices 524
2. Lorentzian Constructions for the Leech Lattice 525

Chapter 27
The Automorphism Group of the 26-Dimensional Even Unimodular Lorentzian Lattice
J.H. Conway 529

1. Introduction 529
2. The Main Theorem 530

Chapter 28
Leech Roots and Vinberg Groups
J.H. Conway and N.J.A. Sloane 534

1. The Leech Roots 534
2. Enumeration of the Leech Roots 543
3. The Lattices $\mathrm{I}_{n,1}$ for $n \leqslant 19$ 549
4. Vinberg's Algorithm and the Initial Batches of Fundamental Roots 549
5. The Later Batches of Fundamental Roots 552

Chapter 29
The Monster Group and its 196884-Dimensional Space
J.H. Conway 556

1. Introduction 556
2. The Golay Code $\mathcal{C}$ and the Parker Loop $\mathcal{P}$ 558
3. The Mathieu Group M_{24}; the Standard Automorphisms of $\mathcal{P}$ 558
4. The Golay Cocode $\mathcal{C}^*$ and the Diagonal Automorphisms ... 558
5. The Group N of Triple Maps 559
6. The Kernel K and the Homomorphism $g \to \bar{g}$ 559
7. The Structures of Various Subgroups of $\overline{N}$ 559
8. The Leech Lattice Λ_{24} and the Group $\overline{Q}_x$ 560
9. Short Elements 561
10. The Basic Representations of N_x 561
11. The Dictionary 562
12. The Algebra 563
13. The Definition of the Monster Group $\overline{G}$, and its Finiteness 563
14. Identifying the Monster 564

Appendix 1. Computing in $\mathcal{P}$ 565
Appendix 2. A Construction for $\mathcal{P}$ 565
Appendix 3. Some Relations in Q_x 566
Appendix 4. Constructing Representations for N_x 568
Appendix 5. Building the Group $\overline{G}_x$ 569

Chapter 30
A Monster Lie Algebra?
R.E. Borcherds, J.H. Conway, L. Queen and N.J.A. Sloane 570

Bibliography 574

Supplementary Bibliography 642

Index 681