

Contents

Introduction — V

- 1 Generic-case complexity in group theory — 1**
 - 1.1 Introduction — 1
 - 1.2 Definition(s) of generic-case complexity — 4
 - 1.2.1 The original definition of generic-case complexity — 4
 - 1.2.2 Weaknesses of the asymptotic density approach to genericity — 7
 - 1.3 Decision problems in group theory: general set-up — 10
 - 1.4 Quotient test methods — 11
 - 1.4.1 Quotient tests and the word problem — 11
 - 1.4.2 Quotient tests and the conjugacy problem — 14
 - 1.4.3 Morseness of generic subgroups and the membership problem — 17
 - 1.4.4 Finer generic conjugacy problem methods — 21
 - 1.5 Generic-case complexity of “search” group-theoretic problems — 23
 - 1.5.1 The word search problem and random van Kampen diagrams — 23
 - 1.5.2 The conjugacy search problem — 25
 - 1.5.3 The membership search problem — 27
 - 1.6 Algorithmically finite groups — 28
 - 1.7 Whitehead algorithm and related problems — 30
 - 1.7.1 Whitehead algorithm and the automorphism problem — 30
 - 1.7.2 Generic-case behavior of Whitehead’s algorithm — 32
 - 1.7.3 Whitehead algorithm for subgroups — 33
 - 1.7.4 Garside algorithm for the conjugacy problem in braid groups — 35
 - 1.8 Generic-case complexity of the isomorphism problem — 38
 - 1.8.1 Generic one-relator groups — 38
 - 1.8.2 Generic quotients of the modular group — 40
 - 1.8.3 Other consequences of isomorphism rigidity — 41

- 2 Random presentations and random subgroups — 45**
 - 2.1 Introduction — 45
 - 2.1.1 Discrete representations — 45
 - 2.1.2 Models of randomness — 47
 - 2.2 Random finite presentations — 48
 - 2.2.1 The density model — 48
 - 2.2.2 The few-relators model — 53
 - 2.2.3 One-relator groups — 55
 - 2.2.4 Rigidity properties — 57
 - 2.2.5 Nilpotent groups — 58

2.3	Random subgroups —	61
2.3.1	Stallings graph of a subgroup —	62
2.3.2	The central tree property and its consequences —	63
2.3.3	Random Stallings graphs —	65
2.3.4	Whitehead minimality —	69
2.3.5	Random subgroups of nonfree groups —	70
2.4	Nonuniform distributions —	71
2.4.1	Prefix-heavy distributions —	72
2.4.2	Markovian automata —	73
3	Randomness and computation in linear groups —	77
3.1	What is a random element of an infinite matrix group? —	77
3.1.1	Random walks —	79
3.1.2	Random subgroups —	80
3.2	Properties of generic elements —	80
3.2.1	The easy case: $SL(2, \mathbb{Z})$ —	80
3.2.2	Random products of matrices in the symplectic and special linear groups —	83
3.2.3	Stronger irreducibility —	84
3.3	Random walks on groups and graphs —	84
3.4	Fourier transform on finite groups —	85
3.5	Fourier estimates via linear algebra —	87
3.5.1	Proof of Theorem 3.5.3 —	88
3.6	Some remarks on matrix norms —	89
3.7	Properties of random subgroups —	90
3.7.1	A guide to the rest of the section —	90
3.8	Subgroups of $SL_2(\mathbb{Z})$ —	92
3.9	Subgroups of $SL_n(\mathbb{Z})$ for $n > 2$ —	97
3.9.1	Ping-pong —	97
3.9.2	ϵ -contraction in $SL_n(\mathbb{Z})$ where $n > 2$ —	99
3.9.3	Proof of Theorem 3.7.1 —	102
3.10	Well-roundedness —	109
3.11	Lyapunov exponent estimates —	112
3.12	How to pick a random element? —	114
3.12.1	How to produce random numbers with a given density? —	115
3.13	Geometric preliminaries —	115
3.13.1	Uniform random points in balls —	115
3.13.2	Computing a random integer matrix —	116
3.14	Action of $SL(2, \mathbb{R})$ and $SL(2, \mathbb{Z})$ on the upper half-plane —	117
3.14.1	Translation distance —	118
3.14.2	The fundamental domain and orbits of the $SL(2, \mathbb{Z})$ action —	118
3.15	Selecting a random element of $SL(2, \mathbb{Z})$ almost uniformly —	120

- 3.15.1 Complexity estimates and implementation — **121**
- 3.16 Extensions to other Fuchsian and Kleinian groups — **122**
- 3.16.1 Constructing the fundamental domain — **122**
- 3.17 Higher rank — **123**
- 3.17.1 $SL(n, \mathbb{Z})$ — **123**
- 3.17.2 $Sp(2n, \mathbb{Z})$ — **124**
- 3.18 Miscellaneous other groups — **125**
- 3.18.1 The orthogonal group — **125**
- 3.18.2 Finite linear groups — **127**
- 3.18.3 $SL(n, \mathbb{R})$ — **127**
- 3.18.4 Other groups? — **128**
- 3.19 Checking Zariski density — **129**
- 3.20 Algorithms for large Galois groups — **131**
- 3.21 Probabilistic algorithms — **133**
- 3.22 Probabilistic algorithm to check if $p(x)$ of degree n has Galois group S_n — **134**
- 3.22.1 Some remarks on the running time of detecting Galois group S_n — **136**
- 3.22.2 Deciding whether the Galois group of a reciprocal polynomial is the hyperoctahedral group — **137**
- 3.23 Back to Zariski density — **138**
- 3.23.1 Testing irreducibility — **138**
- 3.24 A short history of Galois group algorithms — **139**
- 3.24.1 Kronecker's algorithm — **139**
- 3.24.2 Stauduhar's algorithm — **140**
- 3.24.3 Polynomial time (sometimes) — **141**
- 3.25 Some lemmas on permutations — **143**
- 3.25.1 Jordan's theorem — **145**
- 3.26 A bit about polynomials — **146**
- 3.27 The Frobenius density theorem — **146**
- 3.28 Another Zariski density algorithm — **148**
- 3.29 The base case: rank 1 — **149**
- 3.30 Higher rank — **150**
- 3.31 Thin or not? — **150**
- 3.31.1 Computing the fundamental polyhedron — **151**
- 3.31.2 Eigenvalues — **151**
- 3.31.3 Asymptotic eigenvalue distribution — **152**
- 3.31.4 Finite quotients — **153**
- 4 Compression techniques in group theory — 155**
- 4.1 Introduction — **155**
- 4.2 General notations — **158**
- 4.3 Background from complexity theory — **159**

4.4	Rewrite systems — 162
4.5	Groups and the word problem — 163
4.5.1	Presentations for groups — 163
4.5.2	The word problem — 164
4.5.3	HNN-extensions — 166
4.5.4	The Dehn function — 167
4.6	Exponential compression — 168
4.6.1	Motivation: the word problem for $\text{Aut}(F_3)$ — 169
4.6.2	Straight-line programs — 170
4.6.3	Jež's algorithm for equality checking — 171
4.6.4	Cutting out factors from SLPs — 182
4.6.5	The compressed word problem — 184
4.6.6	Complexity of compressed word problems — 186
4.6.7	Power word problems — 192
4.6.8	Further applications of straight-line programs in group theory — 194
4.7	Tower compression and beyond — 199
4.7.1	Motivation: the word problem for the Baumslag group — 199
4.7.2	Power circuits — 201
4.7.3	Solving word problems using power circuits — 214
4.7.4	Ackermannian compression — 218
4.8	Open problems — 220
5	Discrete optimization in groups — 223
5.1	Introduction — 223
5.1.1	Motivation, general set-up, notable results — 223
5.1.2	Brief overview of the problems — 224
5.1.3	Preliminaries: algorithmic set-up — 231
5.1.4	Preliminaries: complexity classes — 233
5.1.5	Preliminaries: nilpotent groups — 235
5.1.6	Preliminaries: hyperbolic groups — 237
5.1.7	Preliminaries: graph groups and virtually special groups — 239
5.1.8	Preliminaries: automaton groups — 240
5.1.9	Preliminaries: wreath products — 240
5.1.10	Preliminaries: polycyclic groups, metabelian groups, Fox derivatives — 241
5.2	Subset sum problem and related problems — 246
5.2.1	Definition — 246
5.2.2	Examples and basic properties — 248
5.2.3	Easy SSP — 250
5.2.4	Distortion as a source of hardness of SSP — 254
5.2.5	Large abelian subgroups as a source of hardness — 260
5.2.6	Mikhailova's construction as a source of hardness — 262

- 5.2.7 Transfer results for **SSP** and related problems — 265
- 5.3 Knapsack problem — 271
- 5.3.1 Definition — 271
- 5.3.2 Groups with semilinear solution to **KP** — 273
- 5.3.3 Right-angled Artin groups — 281
- 5.3.4 Hardness from Diophantine equations — 283
- 5.3.5 Transfer results — 286
- 5.4 Post correspondence problem — 291
- 5.4.1 Connections of **PCP** to group theory — 291
- 5.4.2 Hereditary word problem and **GPCP** — 293
- 5.4.3 **PCP** in nilpotent groups — 297
- 5.4.4 General lemmas and remarks — 302
- 5.4.5 Post correspondence and equalizer problems in metabelian groups — 306
- 5.4.6 Post correspondence and equalizer problems for polycyclic groups — 312

- 6 Problems in group theory motivated by cryptography — 317**
- 6.1 Introduction — 317
- 6.2 The Diffie–Hellman key exchange protocol — 318
- 6.2.1 The ElGamal cryptosystem — 320
- 6.3 The conjugacy problem — 320
- 6.3.1 The Anshel–Anshel–Goldfeld key exchange protocol — 322
- 6.3.2 The twisted conjugacy problem — 324
- 6.4 The decomposition problem — 324
- 6.4.1 “Twisted” protocol — 325
- 6.4.2 Finding intersection of given subgroups — 326
- 6.4.3 Commutative subgroups — 327
- 6.4.4 The factorization problem — 327
- 6.5 The word problem — 328
- 6.5.1 Encryption emulation attack — 329
- 6.5.2 Encryption — 331
- 6.6 The subgroup membership problem — 332
- 6.6.1 Security assumption — 334
- 6.6.2 Trapdoor — 334
- 6.7 Using the subgroup membership decision problem — 334
- 6.8 The isomorphism inversion problem — 335
- 6.9 Semidirect product of groups and more peculiar computational assumptions — 339
- 6.10 The subset sum problem and the knapsack problem — 342
- 6.11 The hidden subgroup problem — 344
- 6.12 Relations between some of the problems — 345

XII — Contents

Bibliography — 349

Index — 371