ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Computation with finitely presented groups

CHARLES C. SIMS

Rutgers University

CAMBRIDGE
UNIVERSITY PRESS

Contents

Preface		*page* xi
Introduction		1
1	**Basic concepts**	6
1.1	Set-theoretic preliminaries	6
1.2	Monoids	8
1.3	Groups	15
1.4	Presentations	18
1.5	Computability	26
1.6	Procedure descriptions	29
1.7	The integers	33
1.8	Backtrack searches	35
1.9	Historical notes	40
2	**Rewriting systems**	43
2.1	Orderings of free monoids	43
2.2	Canonical forms	51
2.3	A test for confluence	57
2.4	Rewriting strategies	66
2.5	The Knuth-Bendix procedure	68
2.6	A second version	76
2.7	Some useful heuristics	83
2.8	Right congruences	88
3	**Automata and rational languages**	96
3.1	Languages	97
3.2	Automata	100
3.3	Automata, continued	108
3.4	The subset construction	111
3.5	Index automata	112
3.6	Trim automata	120
3.7	Minimal automata	126

3.8	Standard automata	130
3.9	Additional constructions	141
3.10	More rewriting applications	147
4	**Subgroups of free products of cyclic groups**	151
4.1	Niladic rewriting systems	151
4.2	Subgroups and their languages	159
4.3	Important cosets	162
4.4	Coset automata	171
4.5	Basic coset enumeration	175
4.6	The coincidence procedure	187
4.7	Standardization in place	192
4.8	Computation with subgroups	196
4.9	Standard coset tables	203
*4.10	Other methods	210
*4.11	General niladic systems	212
5	**Coset enumeration**	217
5.1	The general case	217
5.2	The HLT strategy	227
5.3	The Felsch strategy	232
5.4	Standardizing strategies	239
5.5	Ten versions	245
5.6	Low-index subgroups	251
5.7	Other applications	260
5.8	A comparison with the Knuth-Bendix procedure	264
5.9	Historical notes	266
6	**The Reidemeister-Schreier procedure**	268
6.1	Presentations of subgroups	268
6.2	Examples of extended coset enumeration	276
6.3	An extended HLT enumeration procedure	283
6.4	Simplifying presentations	290
6.5	Historical notes	294
***7**	**Generalized automata**	296
*7.1	Definitions	297
*7.2	Generalized coset automata	301
*7.3	Basic operations	308
*7.4	Some examples	314
8	**Abelian groups**	319
8.1	Free abelian groups	320
8.2	Elementary matrices	330
8.3	Finitely generated abelian groups	332
8.4	Modular techniques	339

8.5 The Kannan-Bachem algorithm 349
8.6 Lattice reduction 360
8.7 The modified LLL algorithm 372
8.8 A comparison 378
8.9 Historical notes 381

9 Polycyclic groups 383
9.1 Commutator subgroups 384
9.2 Solvable and nilpotent groups 386
9.3 Polycyclic groups 390
9.4 Polycyclic presentations 394
9.5 Subgroups 406
9.6 Homomorphisms 414
9.7 Conjugacy in nilpotent groups 417
9.8 Cyclic extensions 419
9.9 Consistency, the nilpotent case 430
9.10 Free nilpotent groups 436
9.11 p-Groups 445

10 Module bases 448
10.1 Ideals in $\mathbb{Z}[X]$ 449
10.2 Modules over $\mathbb{Z}[X]$ 455
10.3 Modules over $\mathbb{Z}[X, Y]$ 467
10.4 The total degree ordering 471
10.5 The Gröbner basis approach 482
10.6 Gröbner bases 488
10.7 Rings of Laurent polynomials 495
10.8 Group rings 507
10.9 Historical notes 512

11 Quotient groups 514
11.1 Describing quotient groups 514
11.2 Abelian quotients 517
11.3 Extensions of modules 524
11.4 Class 2 quotients 535
11.5 Other nilpotent quotients 545
11.6 Metabelian quotients 556
11.7 Enforcing exponent laws 561
11.8 Verifying polycyclicity 568
11.9 Historical notes 569

Appendix: Implementation issues 570
Bibliography 581
Index 597