This series is devoted to thorough yet reasonably concise treatments of topics in any branch of mathematics. Typically, a Tract takes up a single thread in a wide subject and follows its ramifications, throwing light on various of its aspects. Tracts are expected to be rigorous, definitive, and of lasting value to the mathematicians working in the relevant disciplines. Exercises can be included to illustrate techniques, summarize past work, and enhance the book's value as a seminar text. All volumes are properly edited and type-set and are published, initially at least, in hardcover.

Ákos Seress is a Professor of Mathematics at The Ohio State University.

CAMBRIDGE TRACTS IN MATHEMATICS

GENERAL EDITORS
B.BOLLOBAS, W.FULTON, A.KATOK, F.KIRWAN, P.SARNAK

A complete list of the series can be found at http://www.cambridge.org
Recent titles include the following:

115. An Introduction to Hp Spaces (2nd ed.).By P.Koosis
116. Matrices of Sign-Solvable Linear Systems.By R.A.Brualdi and B.L.Shader
117. Generalized Topological Degree and Semilinear Equations.By W .Petryshyn
118. Sets of Multiples.By R.R.Hall
119. Continuum Percolation.By R.Meester and R.Roy
120. Function Spaces, Entropy Numbers and Differential Operators.By D.E.Edmunds and H.Triebel
121. Lévy Processes.By J.Bertoin
122. Duality in Analytic Number Theory.By P.D.T.A.Elliott
123. Ends of Complexes.By A.Ranicki and B.Hughes
124. 3-Transposition Groups.By M.Aschbacher
125. The Hardy-Littlewood Method (2nd ed.).By R.C.Vaughan
126. Dynamical Systems and Semisimple Groups.By R.Feres
127. Spectral Theory of the Riemann Zeta-Function.By Y.Motohashi
128. Introduction to Maximum Principles.By L.E.Fraenkel
129. Gaussian Hilbert Spaces.By S.Janson
130. Automorphic Forms on SL_2 (R).By A.Borel
131. Bipartite Graphs and Their Applications.By A.Asratian, T.Denley, and R.Häggkvist
132. Mixed Hodge Structures and Singularities.By V.Kulikov
133. Multiplicities and Chern Classes in Local Algebra.By P.Roberts
134. Birational Geometry of Algebraic Varieties.By J.Kollár and S.Mori
135. Solutions.By T.Miwa, M.Jimbo, and E.Date
136. Character Sums with Exponential Functions and Their Applications.By S.Konyagin and I.Shparlinski
137. Metric Diophantine Approximation on Manifolds.By V.I.Bernik and M.M.Dodson
138. Random Walks on Infinite Graphs and Groups.By Wolfgang Woess
139. Measure-Preserving Homeomorphisms.By Steve Alpern and V.S.Prasad
140. Derivation and Integration.By Washek F.Pfeffer
141. Fixed Point Theory and Applications.By Ravi P.Agarwal, Maria Meehan,and Donal O'Regan
142. Harmonic Maps between Riemannian Polyhedra.By James Eells and Bent Fuglede
143. Analysis on Fractals.By Jun Kigami
144. Torsors and Rational Points.By A.Skorobogatov
145. Isoperimetric Inequalities.By Isaac Chavel
146. Restricted Orbit Equivalence for Actions of Discrete Amenable Groups.By J.Kammeyer and D.Rudolph
147. Floer Homology Groups in Yang-Mills Theory.By S.K.Donaldson
149. Cohomology of Vector Bundles and Syzygies.By Jerzy Weyman
150. Harmonic Maps, Conservation Laws and Moving Frames.By Frédéric Hélein
151. Frobenius Manifolds and Moduli Spaces for Singularities.By Claus Hertling

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org

ISBN 978-0-521-66103-4

9 780521 661034 >

1 Introduction *page* **1**

1.1 A List of Algorithms 4

1.2 Notation and Terminology 6

1.2.1 Groups 7

1.2.2 Permutation Groups 9

1.2.3 Algorithmic Concepts 10

1.2.4 Graphs 11

1.3 Classification of Randomized Algorithms 12

2 Black-Box Groups 16

2.1 Closure Algorithms 18

2.1.1 Orbit Computations 18

2.1.2 Closure of Algebraic Structures 23

2.2 Random Elements of Black-Box Groups 24

2.3 Random Subproducts 30

2.3.1 Definition and Basic Properties 30

2.3.2 Reducing the Number of Generators 33

2.3.3 Closure Algorithms without Membership Testing 37

2.3.4 Derived and Lower Central Series 38

2.4 Random Prefixes 40

2.4.1 Definition and Basic Properties 40

2.4.2 Applications 44

3 Permutation Groups: A Complexity Overview 48

3.1 Polynomial-Time Algorithms 48

3.2 Nearly Linear-Time Algorithms 51

3.3 Non-Polynomial-Time Methods 52

4 Bases and Strong Generating Sets **55**
4.1 Basic Definitions 55
4.2 The Schreier–Sims Algorithm 57
4.3 The Power of Randomization 62
4.4 Shallow Schreier Trees 64
4.5 Strong Generators in Nearly Linear Time 70
4.5.1 Implementation 75

5 Further Low-Level Algorithms **79**
5.1 Consequences of the Schreier–Sims Method 79
5.1.1 Pointwise Stabilizers 79
5.1.2 Homomorphisms 80
5.1.3 Transitive Constituent and Block Homomorphisms 81
5.1.4 Closures and Normal Closures 83
5.2 Working with Base Images 84
5.3 Permutation Groups as Black-Box Groups 93
5.4 Base Change 97
5.5 Blocks of Imprimitivity 100
5.5.1 Blocks in Nearly Linear Time 101
5.5.2 The Smallest Block Containing a Given Subset 107
5.5.3 Structure Forests 111

6 A Library of Nearly Linear-Time Algorithms **114**
6.1 A Special Case of Group Intersection and Applications 115
6.1.1 Intersection with a Normal Closure 115
6.1.2 Centralizer in the Symmetric Group 117
6.1.3 The Center 120
6.1.4 Centralizer of a Normal Subgroup 120
6.1.5 Core of a Subnormal Subgroup 124
6.2 Composition Series 125
6.2.1 Reduction to the Primitive Case 126
6.2.2 The O'Nan–Scott Theorem 129
6.2.3 Normal Subgroups with Nontrivial Centralizer 133
6.2.4 Groups with a Unique Nonabelian Minimal Normal Subgroup 139
6.2.5 Implementation 146
6.2.6 An Elementary Version 149
6.2.7 Chief Series 155
6.3 Quotients with Small Permutation Degree 156
6.3.1 Solvable Radical and *p*-Core 157

7 Solvable Permutation Groups **162**
7.1 Strong Generators in Solvable Groups 162
7.2 Power-Conjugate Presentations 165
7.3 Working with Elementary Abelian Layers 166
7.3.1 Sylow Subgroups 167
7.3.2 Conjugacy Classes in Solvable Groups 172
7.4 Two Algorithms for Nilpotent Groups 175
7.4.1 A Fast Nilpotency Test 176
7.4.2 The Upper Central Series in Nilpotent Groups 179

8 Strong Generating Tests **183**
8.1 The Schreier–Todd–Coxeter–Sims Procedure 184
8.1.1 Coset Enumeration 184
8.1.2 Leon's Algorithm 186
8.2 Sims's Verify Routine 188
8.3 Toward Strong Generators by a Las Vegas Algorithm 191
8.4 A Short Presentation 197

9 Backtrack Methods **201**
9.1 Traditional Backtrack 202
9.1.1 Pruning the Search Tree: Problem-Independent Methods 203
9.1.2 Pruning the Search Tree: Problem-Dependent Methods 205
9.2 The Partition Method 207
9.3 Normalizers 211
9.4 Conjugacy Classes 214

10 Large-Base Groups **218**
10.1 Labeled Branchings 218
10.1.1 Construction 222
10.2 Alternating and Symmetric Groups 225
10.2.1 Number Theoretic and Probabilistic Estimates 228
10.2.2 Constructive Recognition: Finding the New Generators 235
10.2.3 Constructive Recognition: The Homomorphism λ 239
10.2.4 Constructive Recognition: The Case of Giants 244
10.3 A Randomized Strong Generator Construction 246

Bibliography 254

Index 262