Ákos Seress
The Ohio State University

Permutation Group Algorithms

CAMBRIDGE UNIVERSITY PRESS
## Contents

1 Introduction
   1.1 A List of Algorithms  
   1.2 Notation and Terminology
      1.2.1 Groups  
      1.2.2 Permutation Groups  
      1.2.3 Algorithmic Concepts  
      1.2.4 Graphs  
   1.3 Classification of Randomized Algorithms  

2 Black-Box Groups
   2.1 Closure Algorithms
      2.1.1 Orbit Computations  
      2.1.2 Closure of Algebraic Structures  
   2.2 Random Elements of Black-Box Groups  
   2.3 Random Subproducts
      2.3.1 Definition and Basic Properties  
      2.3.2 Reducing the Number of Generators  
      2.3.3 Closure Algorithms without Membership Testing  
      2.3.4 Derived and Lower Central Series  
   2.4 Random Prefixes
      2.4.1 Definition and Basic Properties  
      2.4.2 Applications  

3 Permutation Groups: A Complexity Overview
   3.1 Polynomial-Time Algorithms  
   3.2 Nearly Linear-Time Algorithms  
   3.3 Non-Polynomial-Time Methods
Contents

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
## Contents

### Solvable Permutation Groups

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

### Strong Generating Tests

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

### Backtrack Methods

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

### Large-Base Groups

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 \( \lambda \) 239  
  10.2.4 Constructive Recognition: The Case of Giants 244  
10.3 A Randomized Strong Generator Construction 246

Bibliography 254

Index 262