

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

136

Christoph M. Hoffmann

Group-Theoretic Algorithms
and Graph Isomorphism



Springer-Verlag
Berlin Heidelberg New York 1982

Editorial Board

W. Brauer P. Brinch Hansen D. Gries C. Moler G. Seegmüller
J. Stoer N. Wirth

Author

Christoph M. Hoffmann
Purdue University, Dept. of Computer Science
West Lafayette, IN 47907, USA

CR Subject Classifications (1979): 3.15, 5.7, 5.9, 5.32

ISBN 3-540-11493-9 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-11493-9 Springer-Verlag New York Heidelberg Berlin

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to "Verwertungsgesellschaft Wort", Munich.

© by Springer-Verlag Berlin Heidelberg 1982
Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2145/3140-543210

PREFACE

This monograph develops the recent algebraic approach to Graph Isomorphism and some of its implications for Computational Complexity. Graph Isomorphism can be rephrased as a purely algebraic problem that exposes a surprising structural similarity with a number of problems in Group Theory. These problems are easily shown to be in **NP** but are not likely **NP**-complete. Moreover, there is a good possibility that they are harder than Graph Isomorphism, with respect to polynomial time reduction. Because of this possibility, the algebraic approach detailed in this book could prove to be very important for Computational Complexity.

The roots of this approach predate Babai's Colored Graph Automorphism Problem and my investigation of cone graphs. Nevertheless, these two papers appear to have been the stimulus leading to the break-through subexponential isomorphism test for trivalent graphs by Furst, Hopcroft and Luks. That paper already contained many of the techniques applied later by Luks in his polynomial time isomorphism test for graphs of fixed valence, most notably the inductive approach to determining automorphisms. Luks' contributions have been primarily a novel way for exploiting the imprimitivity structure of certain permutation groups and his analysis of the structure of the automorphism groups of graphs of fixed valence.

I give my thanks to Juris Hartmanis for suggesting that this material be brought together into a systematic survey of the area as it is at present. John Hopcroft's dedication to Computer Science has been exemplary. I wish to thank him for his willingness to introduce me to Graph Isomorphism. Charles Sims has been my tutor in the mathematical aspects of this work and has been one of those rare individuals willing to carefully read the manuscript and make suggestions for improvement. Paul Young has been exceptionally willing to listen to my ideas and patient enough to criticize them. Francine Berman contributed by partially relieving my teaching load. Merrick Furst and Michael O'Donnell have thoroughly read the manuscript and improved it. I wish to thank them all.

It is a pleasure to acknowledge the support of the National Science Foundation (Grant Nr. MCS 78-01812) which furthered this work. Moreover, the text processing facilities of the Department of Computer Sciences at Purdue University have been crucial for a timely completion.

CONTENTS

Chapter I: Introduction	1
1. Graph Isomorphism	2
2. Computational Complexity	4
3. Group-Theoretic Algorithms	7
4. Background	9
5. Notes and References	10
Chapter II: Basic Concepts	12
1. Review of Elementary Group Theory	12
1.1. Subgroups, Cosets, Lagrange's Theorem	14
1.2. Normal Subgroups, Homomorphism, Isomorphism, and Automorphism	15
1.3. Permutation Groups	16
1.4. Generators, Orbits, and Stabilizers	18
1.5. Direct Products	20
2. Graph Isomorphism and Graph Automorphisms	20
2.1. Isomorphisms as Coset of the Automorphism Group	21
2.2. Some Isomorphism Complete Problems	24
2.3. Graph Isomorphism and Group Intersection	30
3. Computationally Useful Group Descriptions	32
3.1. Determination of a Permutation Group from Generators	32
3.2. A Worked Example	41
3.3. Improvements to Algorithm 3	43
4. Accessible Subgroups	50
5. Notes and References	58

Chapter III: Labelled Graph Automorphisms, Cone Graphs, and p-Groups	60
1. The Labelled Graph Automorphism Problem	60
1.1. A Deterministic Algorithm for Problem 1	61
1.2. A Random Algorithm	66
2. Cone Graphs and Regular Cone Graphs	72
2.1. The Structure of the Automorphism Group of Cone Graphs of Fixed Degree	76
3. p-Groups and Cone Graphs	85
3.1. Sylow p-Subgroups and Properties of p-Groups	86
3.2. Wreath Products and Sylow p-Subgroups of S_n	87
3.3. Imprimitivity of p-Groups	91
3.4. The Central Series	100
3.5. Setwise Stabilizers in p-Groups (Method 1)	108
4. Notes and References	112
 Chapter IV: Isomorphism of Trivalent Graphs and of Cone Graphs of Degree Two	 114
1. The Basic Approach	115
1.1. Properties of the Automorphism Group	115
1.2. Overall Structure of the Algorithm	117
1.3. Reduction to the Setwise Stabilizer in a 2-Group	119
1.4. Binary Cone Graphs	124
2. An Algorithm for Determining the Automorphisms of Trivalent Graphs	125
3. Setwise Stabilizers in p-Groups (Method 2)	129
3.1. The Algorithm	131
3.2. Analysis of Algorithm 2	136
4. An $O(n^4)$ Isomorphism Test for Trivalent Graphs	138
4.1. Improved Algorithms for p-Groups	139
4.2. The Imprimitivity Problem for 2-Groups	157
4.3. Gadgets for Trivalent Graph Isomorphism	167
5. Notes and References	176

Chapter V: Graphs of Fixed Valence and Cone Graphs of Fixed Degree	178
1. The Basic Algorithm	179
1.1. Outline of the Method	179
1.2. The Algorithm	181
2. Properties of the Automorphism Group	184
3. Setwise Stabilizers in the Class Γ_b	188
3.1. Outline of the Method	189
3.2. Group-Theoretic Preliminaries	193
3.3. The Socle of Primitive Groups	199
3.4. Primitive Groups with Nonabelian Socle	205
3.5. Primitive Groups with Abelian Socle	210
3.6. The Algorithm	215
4. Remarks	227
5. Notes and References	229
 Chapter VI: Group-Theoretic Problems	 231
1. Some Combinatorial Problems as Group-Theoretic Problems	231
2. Group-Theoretic Problems of Intermediate Difficulty	235
2.1. Double Coset Problems	236
2.2. Intersection Problems	238
2.3. Miscellaneous Problems	241
2.4. Isomorphism Complete Problems	245
2.5. Remarks	245
3. A Problem with a Short Verifiable Solution	246
4. Subproblems in \mathbf{P}	248
4.1. Group Intersection Problems	248
4.2. Centralizer and Center	252
4.3. An Automorphism Restriction Problem	260
5. Normal Closure, Commutator Subgroups, Solvability, and Nilpotence	261
5.1. Normal Closure	262
5.2. Commutators and Commutator Groups	265
5.3. Testing Solvability and Nilpotence	268
6. Open Problems	270
7. Notes and References	271

Bibliography	273
Indices	296
1. Problem Index	296
2. Algorithm Index	298
3. Definition Index	299
4. Lemma Index	302
5. Proposition Index	305
6. Theorem Index	307
7. Corollary Index	310