

Lecture Notes in Artificial Intelligence 1095

Subseries of Lecture Notes in Computer Science

Edited by J. G. Carbonell and J. Siekmann

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

W. McCune R. Padmanabhan

Automated Deduction in Equational Logic and Cubic Curves



Springer

Series Editors

Jaime G. Carbonell, Carnegie Mellon University, Pittsburgh, PA, USA

Jörg Siekmann, University of Saarland, Saarbrücken, Germany

Authors

W. McCune

Mathematics and Computer Science Division, Argonne National Laboratory
Argonne, Illinois 60439, USA

R. Padmanabhan

Department of Mathematics, University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

MacCune, William:

Automated deduction in equational logic and cubic curves / W.
Mc Cune ; R. Padmanabhan. - Berlin ; Heidelberg ; New York
; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ;
Santa Clara ; Singapore ; Tokyo : Springer, 1996

(Lecture notes in computer science ; Vol. 1095 : Lecture notes in
artificial intelligence)

ISBN 3-540-61398-6

NE: Padmanabhan, R.; GT

CR Subject Classification (1991): I.2.3, F.4.1, I.3.5

1991 Mathematics Subject Classification: 03B35, 03C05, 14Q05

ISBN 3-540-61398-6 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1996

Printed in Germany

Typesetting: Camera ready by author

SPIN 10513209 06/3142 ~ 5 4 3 2 1 0 Printed on acid-free paper

Preface

The aim of this monograph is to demonstrate that automated deduction is starting to become a practical tool for working mathematicians. It contains a set of problems and theorems that arose in correspondence between the authors starting early in 1993. One of us (Padmanabhan), a mathematician working in universal algebra and geometry, contacted the other (McCune), a computer scientist working in automated deduction, after reading a survey article by Larry Wos on applications of automated reasoning [80]. Padmanabhan sent McCune a few first-order theorems and asked whether Argonne's theorem prover Otter could prove them. Otter succeeded and, in a few cases, found slightly better results. The collaboration quickly took off.

We worked mostly in four areas: (1) equational proofs of theorems that had been proved previously with higher-order arguments, (2) a new equational inference rule for problems about cubic curves in algebraic geometry, (3) a conjecture about cancellative semigroups, proving many theorems that support the conjecture, and (4) equational bases with particular properties such as single axioms and independent self-dual bases. Some of the results presented here have also appeared (or will also appear) elsewhere in more detail.

The intended audience of this monograph is both mathematicians and computer scientists. We include many new results, and we hope that mathematicians working in equational logic, universal algebra, or algebraic geometry will gain some understanding of the current capabilities of automated deduction (and, of course, we hope that readers will find new practical uses for automated deduction). Computer scientists working in automated reasoning will find a large and varied source of theorems and problems that will be useful in designing and evaluating automated theorem-proving programs and strategies.

Otter (version 3.0.4) and MACE (version 1.2.0) are the two computer programs that made this work possible. Both programs are in the public domain and are available by anonymous FTP and through the World Wide Web (WWW). See either of

`ftp://info.mcs.anl.gov/pub/Otter/README`
`http://www.mcs.anl.gov/home/mccune/ar/`

for information on obtaining the programs. The primary documentation for the programs is [39] and [37, 38]; these are included with the programs when obtained from the above network locations. We also have the WWW document

<http://www.mcs.anl.gov/home/mccune/ar/monograph/>

associated with this work; it points to all of the Otter and MACE input files and proofs to which we refer, and it is particularly useful if the reader wishes to see precisely the search strategy we used or to experiment with related theorems.

Special thanks go to Larry Wos and to Ross Overbeek. Larry introduced the notions of strategy and simplification to automated deduction and invented the inference rule paramodulation for equality; all three of these concepts are at the center of this work. Also, Larry simplified several of our Otter proofs (in one case from 816 steps to 99!) so that they could be included in these pages. Ross is due a lot of the credit for Otter's basic design and high performance, because in building Otter, McCune borrowed so heavily from Ross's earlier theorem provers and ideas. Special thanks also go to Dr. David Kelly (of the University of Manitoba) and Dr. Stanley Burris (of the University of Waterloo) for encouraging Padmanabhan to get in touch with the Argonne group. Padmanabhan thanks Dr. Lynn Margaret Batten and Dr. Peter McClure, successive heads of the Department of Mathematics at the University of Manitoba, for creating a pleasant atmosphere conducive to creative research, without which this project could not have been completed so smoothly. We also thank Dr. Harry Lakser for compiling a Macintosh version of Otter, which enabled Padmanabhan to experiment with some of his conjectures on a Mac. And we are deeply indebted to Gail Pieper, who read several versions of the manuscript and made many improvements in the presentation.

The cubic curves in most of the figures were drawn with data generated by the Pisces software [77] developed at The Geometry Center of the University of Minnesota.

McCune was supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Computational and Technology Research, U.S. Department of Energy, under Contract W-31-109-Eng-38. Padmanabhan was supported by the University of Manitoba and by operating grant #A8215 from NSERC of Canada.

Table of Contents

1. Introduction	1
1.1 Algebras and Equational Logic	2
1.2 Outside of Equational Logic	4
1.3 First-Order and Higher-Order Proofs	4
1.4 Previous Applications of Automated Deduction	6
1.5 Organization	7
2. Otter and MACE	11
2.1 Definitions	11
2.2 Otter	13
2.2.1 The Main Loop	14
2.2.2 General Strategies	15
2.2.3 Equational Problems	19
2.2.4 Equational Problems with the Rule (gL)	20
2.2.5 Conjectures with Deduction Rules	22
2.2.6 Running Otter	23
2.2.7 Example Input Files and Proofs	24
2.2.8 Soundness of Otter	27
2.3 MACE	29
2.3.1 Use of MACE	29
2.3.2 Soundness of MACE	31
3. Algebras over Algebraic Curves	33
3.1 What Is a Uniqueness Theorem?	33
3.1.1 The Rigidity Lemma	33
3.1.2 Applications to Cubic Curves	36
3.2 The Median Law	46
3.3 Abelian Groups	48
3.4 Uniqueness of Group Laws	51
3.5 Uniqueness of n -ary Steiner Laws	54
3.6 Group Laws on a Quartic Curve	59

4. Other (gL)-Algebras	63
4.1 Equations Consistent with (gL)	64
4.1.1 Abelian Groups	64
4.1.2 Quasigroups	69
4.1.3 Boolean Groups	72
4.1.4 Cancellative Semigroups	74
4.2 Theories Strictly Inconsistent with (gL)	77
4.3 Quasigroups and the Overlay Principle	79
4.4 Closure Conditions and (gL)	81
4.5 A Discovery Rule	92
5. Semigroups	95
5.1 A Conjecture in Cancellative Semigroups	95
5.2 Theorems Supporting the Conjecture	96
5.3 Meta-Abelian CS and the Quotient Condition	103
6. Lattice-Like Algebras	109
6.1 Equational Theory of Lattices	109
6.1.1 Quasilattices	111
6.1.2 Weakly Associative Lattices	111
6.1.3 Near Lattices and Transitive Near Lattices	113
6.2 Distributivity and Modularity	113
6.2.1 Lattices	119
6.2.2 Quasilattices	124
6.3 Uniqueness of Operations	133
6.3.1 Lattices	133
6.3.2 Quasilattices	134
6.3.3 Weakly Associative Lattices	135
6.3.4 Transitive Near Lattices	136
6.4 Single Axioms	137
6.4.1 Presence of Jónsson Polynomials	139
6.4.2 A Short Single Axiom for Lattices	143
6.4.3 Weakly Associative Lattices	144
6.5 Boolean Algebras	146
6.5.1 Frink's Theorem	147
6.5.2 Robbins Algebra	148
6.5.3 Ternary Boolean Algebra	152
7. Independent Self-Dual Bases	155
7.1 Self-Dual Bases for Group Theory	156
7.2 Self-Dual Schemas for Subvarieties of GT	160
7.3 Self-Dual Bases for Boolean Algebra	162
7.3.1 Padmanabhan's 6-Basis	163
7.3.2 A 2-Basis from Pixley Reduction	164
7.3.3 A 2-Basis from Majority Reduction	173

7.3.4	A 3-Basis from Majority Reduction	176
8.	Miscellaneous Topics	183
8.1	Inverse Loops and Moufang Loops	183
8.1.1	Bases for Moufang Loops	184
8.1.2	Single Axioms for Inverse Loops and Moufang Loops ..	191
8.2	Quasigroups	198
8.3	Algebras of Set Difference	202
A.	Theorems Proved	207
A.3	Algebras over Algebraic Curves	207
A.4	Other (gL) -Algebras	207
A.5	Semigroups	209
A.6	Lattice-like Algebras	209
A.7	Independent Self-Dual Bases	209
A.8	Miscellaneous Topics	210
B.	Open Questions	211
B.3	Algebras over Algebraic Curves	211
B.4	Other (gL) -Algebras	211
B.5	Semigroups	212
B.6	Lattice-like Algebras	212
B.7	Independent Self-Dual Bases	212
B.8	Miscellaneous Topics	213
C.	The Autonomous Mode	215
	Bibliography	219
	Index	225

List of Figures

3.1	The Median Law	37
3.2	Chord-Tangent Operation on a Cubic Curve	41
3.3	Configuration I for Thm. GEO-1	42
3.4	Configuration II for Thm. GEO-1.....	42
3.5	Desargues Configuration, Thm. GEO-2.....	44
3.6	A Group $\langle G; +, ', e \rangle$ on a Cubic Curve.....	51
3.7	The Conic Construction on a Cubic Curve.....	60
6.1	Nondistributive Lattices	116
6.2	Irreducible Quasilattices	118

List of Tables

1.1	Birkhoff's Inference Rules for Equational Logic.....	3
1.2	Wos's Paramodulation for Equational Logic.....	3
3.1	Examples of Uniqueness of Algebraic Laws.....	34
3.2	Equationally Definable Concepts in Cubic Curves.....	40
4.1	Discovery Rule Examples	94
C.1	Tuned vs. Autonomous Searches on Non- (gL) Theorems	216