Application of Automated Deduction to the Search for Single Axioms for Exponent Groups*

William McCune and Larry Wos
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4801
U.S.A.

e-mail: mccune@mcs.anl.gov, wos@mcs.anl.gov
phone: 708-252-3065 or 312-493-0767

March 30, 1995

Abstract

We present new results in axiomatic group theory obtained by using automated deduction programs. The results include single axioms, some with the identity and others without, for groups of exponents 3, 4, 5, and 7, and a general form for single axioms for groups of odd exponent. The results were obtained by using the programs in three separate ways: as a symbolic calculator, to search for proofs, and to search for counterexamples. We also touch on relations between logic programming and automated reasoning.

1 Introduction

A group of exponent n is a group in which for all elements x, x^n is the identity e. Groups of exponent 2, $xx = e$, are also called Boolean groups. A single axiom for an equational theory is an equality from which the entire theory can be derived by equational reasoning. We are concerned with single axioms for groups of exponent n, $n \geq 2$. B. H. Neumann [6, p.83] gives a general form for single axioms for certain subvarieties of groups, including exponent groups. The axioms it produces are very long, they contain inverse, and they do not contain the identity. We sought shorter axioms without inverse, some without and others with identity. When we started the study, we knew of simple single axioms for Boolean groups [4]. Since then, we have found many single axioms, not containing the identity, for exponents 3, 5, and 7, and a general form for groups of odd exponent. We have also found single axioms, containing the identity, for exponents 2 and 4 and for odd n, $3 \leq n \leq 17$.

We made extensive use of three types of symbolic computation in discovering the axioms. First, the automated deduction program OTTER [1, 2] was used as a symbolic calculator,

*This work was supported by the Applied Mathematical Sciences subprogram of the Office of Energy Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

performing strictly algorithmic deductions, to generate sets of candidate single axioms. We consider such use to be a type of logic programming. Second, OTTER also played its traditional role as a theorem prover, to attempt to show that candidates are in fact single axioms. Third, the program FINDER [7] was used to search for counterexamples, to show that candidates are not single axioms.

The first two types of computation listed above illustrate our view on the relationships between logic programming and automated reasoning [8]. Although the theoretical foundations of the two areas are closely related and the implementation methods can be similar, practical applications are usually far apart, with logic programming relying on algorithmic deduction, and automated reasoning on less-focused search.

Several of the methods we used are based on recent work in which single axioms were discovered for the left group and right group calculi [3] and for several axiomatizations of ordinary groups and Abelian groups [4].

2 Axiomatizations of Exponent Groups

Throughout the paper, e is the group identity, $(x \cdot y)$ is product, x^{-1} is inverse, and x^n is right-associated.

The variety of groups of exponent n, $n \geq 1$, can be axiomatized with the following set of three equalities.

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	associativity	(2.1)
$e \cdot x = x$	left identity	(2.2)
$x^n = e$	exponent property	(2.3)

(Inverse is not required, because $x^{-1} = x^{n-1}$. Also, left identity can be replaced with right identity $x \cdot e = x$.) However, the identity e need not be mentioned, for the following set axiomatizes the same structures.

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	associativity	
$y^n \cdot x = x$	left identity without e	(2.4)
$x^n = y^n$	exponent property without e	(2.5)

(Again, left identity can be replaced with right identity $x \cdot y^n = x$.)

An equality $\alpha = \beta$ is a single axiom for groups of exponent n if and only if it holds in groups of exponent n and one of the above sets can be derived from it. (It is known that either α or β must be a variable.) Note that the mirror image of a single axiom, obtained by flipping arguments of all occurrences of product, is also a single axiom.

3 Programs Used

OTTER is a resolution/paramodulation automated deduction system for first-order logic with equality. As well as its normal role of searching for proofs, OTTER can be "programmed" to perform symbolic computation tasks. We list here examples of tasks that arose during our study of exponent groups and that can be addressed by "programming" OTTER.

- Given a string of terms, construct the set of products of the terms with all possible associations. For example, a string of length 5 produces a set of 14 associations.
- Given term t, construct $\{t' | t'$ can be obtained from t by inserting one occurrence of $e\}$.
- Given a set of equalities, rewrite each with $x^{-1} = x \cdot x \cdot x$; then paramodulate one level from the left argument of $x \cdot x \cdot x \cdot x = e$.
- Given a set of equalities, generate 10,000 consequences of the set; then extract equalities with three distinct variables and one occurrence of e.

The preceding methods and others were used to generate sets of candidate single axioms for exponent groups.

We used OTTER as a theorem prover to attempt to show that candidates are single axioms. The search strategy was based on Knuth-Bendix completion, and it included the following enhancements.

- Equalities that could not be oriented into rewrite rules were allowed to participate in the search.
- We placed a limit on the length of equalities. The limit for each case was typically determined by experimentation.
- We used the ratio strategy [5], which combines best-first search and breadth-first search, for selecting the next equality for application of paramodulation.
- Denials of the associativity, identity, and exponent properties were input, but they did not participate in the searches. They were used only to detect proofs.
- We occasionally pruned the search based on our intuition.

When working on a particular type of candidate, we ran individual OTTER jobs, carefully tuning the strategy. In contrast, with a set of, say, 1000 candidates we would fix the strategy and automatically run a sequence of 1000 OTTER searches, each with a small time limit.

FINDER [7] is a program that searches for models of sets of first-order clauses. Given a candidate, if FINDER produces a model violating a group property or the exponent property, the candidate is not a single axiom. Most of our useful assistance from FINDER was with jobs of less than one minute, finding models of less than five elements.

4 Results

4.1 Single Axioms without the Identity

For groups with exponent 2, we already knew short single axioms [4], for example,

$$((x \cdot y) \cdot z) \cdot (x \cdot z) = y. \tag{4.1}$$

In contrast to (4.1), the axiom produced by B. H. Neumann's general form contains 14 occurrences of product and 9 occurrences of inverse, and we have not been able to verify it with OTTER.

For exponent 3, we quickly found the following, each of which is a single axiom, by considering all associations of $xxxyzzz = y$.

$$x \cdot ((x \cdot (x \cdot (y \cdot (z \cdot z)))) \cdot z) = y \tag{4.2}$$
$$x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot (z \cdot z)) = y \tag{4.3}$$
$$x \cdot ((((x \cdot x) \cdot (y \cdot z)) \cdot z) \cdot z) = y \tag{4.4}$$

For exponent 4, we considered all associations of several strings, but we failed to find short single axioms (without the identity e).

For exponent 5, we found 14 single axioms (excluding mirror images), including the following, by considering associations of $xxxxxyzzzzz = y$.

$$x \cdot (x \cdot ((x \cdot (x \cdot (x \cdot (y \cdot (z \cdot (z \cdot (z \cdot z))))))) \cdot z)) = y \tag{4.5}$$
$$x \cdot (x \cdot ((x \cdot (x \cdot ((x \cdot y) \cdot z))) \cdot (z \cdot (z \cdot (z \cdot z))))) = y \tag{4.6}$$

Odd Exponent Without Identity. We noticed a similarity between (4.2) and (4.5) and conjectured that the following equalities (written without the operator and assuming right association where parentheses are omitted) are single axioms for exponents 7 and 9, respectively.

$$xxx(xxxxyzzzzzz)z = y \qquad \text{exponent 7} \tag{4.7}$$
$$xxxx(xxxxxyzzzzzzzzz)z = y \qquad \text{exponent 9} \tag{4.8}$$

OTTER quickly proved the conjectures. We also verified the obvious general form for odd exponents through 21. We noticed similarities in the OTTER proofs that (4.2), (4.5), (4.7), and (4.8) are single axioms for exponents 3, 5, 7, and 9, respectively, and proved (by hand) that the general form holds for all odd exponents.

We believe that there exists another general form for groups of odd exponent that can be obtained by generalizing (4.3) and (4.6), but we have not yet worked out all the details.

Even Exponent Without Identity. We failed to find any new single axioms for groups of exponent 6 or exponent 8, and we have little intuition about general forms for single axioms for even exponents.

4.2 Single Axioms with Identity

Our main reason for seeking single axioms *with* the identity for exponent groups is that in the case of ordinary groups, single axioms exist in terms of product and inverse, but no single axioms exist in terms of product, inverse, and identity [6]. We believe also that axioms with identity are more natural and appealing.

For exponent 2, we easily found many single axioms with one occurrence of the identity e by considering simple transformations of known single axioms without e. An example is

$$x \cdot ((y \cdot (e \cdot z)) \cdot (x \cdot z)) = y, \tag{4.9}$$

which is also a single axiom for exponent 2 if $(e \cdot z)$ is replaced with z. We conjectured that an equality without e is a single axiom if and only if the result of inserting one occurrence of e in any position is also a single axiom. However, with the assistance of FINDER, we found counterexamples to both directions of the equivalence. Results for exponent 3 were similar to those for exponent 2. A sample single axiom for exponent 3 is

$$x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot (e \cdot (z \cdot z))) = y. \tag{4.10}$$

For exponent 4, we had no single axioms without e to use as a starting point, so we turned to brute force. We considered the 1429 associations of $xxxxyzzzz = y$, and for each of those, the 17 subterms at which an occurrence of e can be inserted. By symmetry we inserted e only to the left of the subterms and had $1429 * 17 = 24293$ candidates, each with one occurrence of e. With each candidate, we ran an OTTER search with a time limit of 30 seconds. (Most searches were terminated in less than 30 seconds by the restrictive search strategy.) One single axiom emerged:

$$x \cdot ((x \cdot ((x \cdot ((e \cdot ((x \cdot y) \cdot z)) \cdot z)) \cdot z)) \cdot z) = y. \tag{4.11}$$

Several of the other candidates derived sufficient properties except for associativity, and when we reran those candidates with a greater time limit, nine more single axioms emerged. Note that in (4.11), none of the products is applied to two products. All single axioms known to us for exponent 4 have that property.

For exponent 6, we considered the set analogous to the exponent 4 candidates and ran OTTER searches with a subset of those, but we failed to find single axioms.

Odd Exponent with Identity. We observed the following relationships between (4.3), (4.6), and (4.10). Equalities (4.3) and (4.10) (both exponent 3) are similar except for e, and (4.6) (exponent 5) has a form similar to (4.3) (exponent 3). By analogy, we conjectured that (written without the operator and assuming right association where parentheses are omitted)

$$xx(xx(xy)z)ezzzz = y \tag{4.12}$$
$$xxx(xxx(xy)z)ezzzzzz = y \tag{4.13}$$

are single axioms for exponents 5 and 7, respectively. OTTER proved the required theorems. We then conjectured that the obvious general form holds for all odd exponents.

OTTER has checked the general form for cases through exponent 17 (the first proof for exponent 17 required 23 hours on a SPARCstation 2 and had 181 steps), but we have not yet worked out the details for the general proof. As in the general forms without e, we are attempting to generalize the OTTER proofs for cases $3, 5, 7, \cdots, 17$ with e, but the OTTER proofs with e are much more complex.

Appendix

We present here an OTTER proof (found in less than 1 second on a SPARCstation 2) that (4.3) is strong enough to be a single axiom for groups of exponent 3. Equalities 88, 99, and 104 below are sufficient properties. The justification $m \rightarrow n$ indicates paramodulation from m into n, and $: m, n, \cdots$ indicates simplification with $m, n, \cdots$.

6	$x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot (z \cdot z)) = y$	[(4.3)]
8	$x \cdot (y \cdot ((z \cdot z) \cdot (z \cdot z))) = (x \cdot y) \cdot z$	[6→6]
10	$(y \cdot (y \cdot ((y \cdot x) \cdot (z \cdot z)))) \cdot z = x$	[6→8]
13	$(x \cdot ((x \cdot (x \cdot y)) \cdot z)) \cdot (z \cdot z) = y$	[8→10]
15	$((x \cdot x) \cdot x) \cdot x = x$	[8→10]
19	$(x \cdot x) \cdot (((x \cdot x) \cdot x) \cdot (x \cdot x)) = x$	[15→6]
23	$(((x \cdot x) \cdot x) \cdot (x \cdot y)) \cdot (y \cdot y) = x$	[15→13:15]
27	$(x \cdot (z \cdot ((z \cdot (z \cdot y)) \cdot (u \cdot u)))) \cdot u = x \cdot y$	[13→8]
29	$(x \cdot x) \cdot (x \cdot ((x \cdot x) \cdot (x \cdot x))) = x$	[19→6]
31	$(x \cdot y) \cdot (((y \cdot y) \cdot (y \cdot y)) \cdot ((y \cdot y) \cdot (y \cdot y))) = x$	[8→23:15]
33	$(x \cdot (((y \cdot y) \cdot y) \cdot (y \cdot (z \cdot z)))) \cdot z = x \cdot y$	[23→8]
40	$(x \cdot (y \cdot z)) \cdot (z \cdot z) = x \cdot y$	[8→33:15]
47	$x \cdot (x \cdot (x \cdot y)) = y$	[13:40]
49	$(x \cdot y) \cdot z = x \cdot (y \cdot ((z \cdot z) \cdot (z \cdot z)))$	[33→27:15,15]
61	$(x \cdot (y \cdot z)) \cdot ((u \cdot u) \cdot (u \cdot u)) = x \cdot (y \cdot (z \cdot u))$	[40→40]
64	$x \cdot ((y \cdot x) \cdot (y \cdot x)) = y \cdot y$	[47→40]
76	$(x \cdot y) \cdot ((y \cdot y) \cdot (y \cdot (y \cdot y))) = x$	[31:61]
80	$(x \cdot x) \cdot (x \cdot x) = x$	[29:64]
88	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[49:80]
99	$x \cdot (y \cdot (y \cdot y)) = x$	[76:88,47,88]
104	$x \cdot (x \cdot x) = y \cdot (y \cdot y)$	[99→47]

References

[1] W. McCune. OTTER 2.0 Users Guide. Tech. Report ANL-90/9, Argonne National Laboratory, Argonne, IL, March 1990.

[2] W. McCune. What's New in OTTER 2.2. Tech. Memo ANL/MCS-TM-153, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, July 1991.

[3] W. McCune. Automated discovery of new axiomatizations of the left group and right group calculi. *Journal of Automated Reasoning*, 9(1):1–24, 1992.

[4] W. McCune. Single axioms for groups and Abelian groups with various operations. *Journal of Automated Reasoning*, 10(1):1–13, 1993.

[5] W. McCune and L. Wos. Experiments in automated deduction with condensed detachment. In D. Kapur, editor, *Proceedings of the 11th International Conference on Automated Deduction, Lecture Notes in Artificial Intelligence, Vol. 607*, pages 209–223, New York, June 1992. Springer-Verlag.

[6] B. H. Neumann. Another single law for groups. *Bull. Australian Math. Soc.*, 23:81–102, 1981.

[7] J. Slaney. FINDER, finite domain enumerator: Version 1.0 notes and guide. Tech. Report TR-ARP-10/91, Automated Reasoning Project, Australian National University, Canberra, Australia, 1991.

[8] L. Wos and W. McCune. Automated theorem proving and logic programming: A natural symbiosis. *Journal of Logic Programming*, 11(1):1–53, July 1991.