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

LPAR '92
July, 1992

Axiomatizations of Exponent Groups

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

An Axiomatization with identity:

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

An Axiomatization without identity:

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

Single Axioms for Exponent 2

Previously known single axioms, without identity, for $x^2 = e$ (Boolean) groups:

$x \cdot ((y \cdot z) \cdot (x \cdot z)) = y$
$(x \cdot y) \cdot (x \cdot (z \cdot y)) = z$
$x \cdot (((x \cdot y) \cdot z) \cdot y) = z$
$((x \cdot y) \cdot (x \cdot z)) \cdot y = z$
$((x \cdot y) \cdot z) \cdot (x \cdot z) = y$
$(x \cdot (y \cdot (x \cdot z))) \cdot z = y$

We easily found many single axioms, with identity, for $x^2 = e$ groups, for example:

$((x \cdot y) \cdot (z \cdot y)) \cdot (x \cdot e) = z$
$x \cdot ((y \cdot (z \cdot (x \cdot e))) \cdot z) = y$
$x \cdot (e \cdot ((x \cdot y) \cdot (z \cdot y))) = z$

Method: consider many transformations on axioms without identity.

An Example Proof

6 $x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot (z \cdot z)) = y$

is a single axiom for exponent 3 groups.
Otter proof (< 1 second):

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]

{88,99,104} is an axiomatization of exponent 3 groups.

Programs Used

- Otter, in symbolic-calculator mode.
- Otter, in proof-search mode.
- Otter-Loop, a simple program that runs a sequence of Otter searches.
- FINDER, to search for counterexamples.

Calculation with Otter

To construct sets of candidate single axioms, we "programmed" Otter to do various tasks, for example:

- Construct all binary associations of a string.
- 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.

Search with Otter

For these experiments, we used a search strategy based on Knuth-Bendix completion.

- Nonorientable equalities participated in the search.
- Limit the size of equalities in the search.
- Combine simplest-first search and breadth-first search when selecting the next equality for application of paramodulation.
- Forward search—denials of associativity, identity, and exponent properties were used only to detect proofs.
- Occasionally prune the search based on intuition.

Otter-Loop

- A very simple UNIX C-shell program.
- Given a set of candidate single axioms, run an Otter search with each candidate.

FINite Domain EnumeratoR

(by John Slaney, Australian National University)

- Searches for small (finite) models of first-order statements.
- We used FINDER to find counterexamples—for example, to find a model of a candidate single axiom that is not associative.

Single Axioms Without Identity

Exponent 3: consider all associations of $xxxyzzz = y$. Results include

$$x \cdot ((x \cdot (x \cdot (y \cdot (z \cdot z)))) \cdot z) = y \quad (4.2)$$
$$x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot (z \cdot z)) = y \quad (4.3)$$
$$x \cdot ((((x \cdot x) \cdot (y \cdot z)) \cdot z) \cdot z) = y \quad (4.4)$$

Exponent 4: failure.

Exponent 5: consider all associations of $xxxxyzzzz = y$. Results include

$$x \cdot (x \cdot ((x \cdot (x \cdot (x \cdot (y \cdot (z \cdot (z \cdot (z \cdot z)))))))) \cdot z)) = y \quad (4.5)$$
$$x \cdot (x \cdot ((x \cdot (x \cdot ((x \cdot y) \cdot z))) \cdot (z \cdot (z \cdot (z \cdot z))))) = y \quad (4.6)$$

Consider (4.2) and (4.5), note similarity, and conjecture axioms for exponents 7 and 9:

$x(xxyzz)z = y$	exponent 3	(4.2)
$xx(xxxyzzzz)z = y$	exponent 5	(4.5)
$xxx(xxxxyzzzzzz)z = y$	exponent 7	(4.7)
$xxxx(xxxxxyzzzzzzzzz)z = y$	exponent 9	(4.8)

Otter quickly proved the conjectures.

We then proved (by hand) that the pattern works for all odd exponents.

Single Axioms With Identity

- As in the case without identity, single axioms for odd exponent were not difficult to find.
- A pattern emerged:

$x(x(xy)z)ezz = y$	exponent 3
$xx(xx(xy)z)ezzzz = y$	exponent 5
$xxx(xxx(xy)z)ezzzzzz = y$	exponent 7
$xxxx(xxxx(xy)z)ezzzzzzzzz = y$	exponent 9

- The pattern has been verified with Otter for odd exponent ≤ 17.
- (The first proof for exponent 17 has 181 steps and required 23 hours on a SPARC 2.)

Single Axioms for Even Exponents

- are much more difficult to find for exponents > 2.
- We have several for exponent 4 with identity, for example,

$$x \cdot ((e \cdot ((x \cdot (x \cdot ((x \cdot (y \cdot z)) \cdot z))) \cdot z)) \cdot z)) = y$$
$$x \cdot ((x \cdot ((e \cdot ((x \cdot (x \cdot (y \cdot z))) \cdot z)) \cdot z)) \cdot z)) = y$$
$$x \cdot ((x \cdot ((x \cdot ((e \cdot ((x \cdot y) \cdot z)) \cdot z)) \cdot z)) \cdot z)) = y$$
$$x \cdot ((e \cdot ((x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot z)) \cdot z)) \cdot z)) = y$$

(Note curious nesting property.)

- For exponent 4 without identity, we can replace e with w^4 to obtain single axioms, but we have not found any with 10 variable occurrences.
- For even exponents > 4, we have not found any single axioms in product and identity or in product alone.

Summary

- Many new results in axiomatic group theory.
- Nonstandard uses of a theorem prover:
  - to build large sets (> 10000) of candidate axioms;
  - to run a large sequence of searches;
  - to search for single axioms as well as search for proofs that candidates are single axioms;
- Use of FINDER to search for counterexamples.
- As users, we had to do (know) very little algebra.