SINGLE AXIOMS: WITH AND WITHOUT COMPUTERS

WILLIAM MCCUNE
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439
USA
E-mail: mccune@mcs.anl.gov
Web: http://www.mcs.anl.gov/~mccune

1 Introduction

This note is an (incomplete) summary of results on single equational axioms for algebraic theories. Pioneering results were obtained decades ago (without the use of computers) by logicians such as Tarski, Higman, Neumann, and Padmanabhan. Use of today's high-speed computers and sophisticated software for searching for proofs and counterexamples has led to many additional results.

Considered here are equationally defined algebras, and the goal is to find simple single equations (1-bases) that axiomatize algebras that are ordinarily presented with sets of equations. For example, a standard way to define group theory is as an algebra with a binary operation, a unary operation, and a constant e satisfying the three equations

$$e \cdot x = x$$
$$x^{-1} \cdot x = e$$
$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

What is the shortest equation, if any, that is equivalent to the preceding 3-basis? Unfortunately, there is no single equational axiom for group theory in terms of product, inverse, and e.[1] However, there are single axioms in terms of product and inverse alone. The shortest is[2]

$$(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u.$$

Although the identity e is not mentioned in the preceding axiom, one can prove that a constant with the appropriate properties exists.

The focus in this note is on group-like algebras such as groups, Abelian groups, Boolean groups, and loops, and on lattice-like algebras such as lattices, weakly associative lattices, and Boolean algebras. Also considered are

nonstandard operations for these algebras. For example, groups can be defined in terms of a single binary operation that can be thought of as division, $x/y = x \cdot y^{-1}$, and Boolean algebra can be defined in terms of just the Sheffer stroke (or NAND), $x|y = x' + y'$. Although a single axiom for group theory in terms of division is not strictly equivalent to the 3-basis above, it is *definitionally* equivalent.

Substantial interest in single axioms also exists for Hilbert-style sentential systems which use modus ponens rather than equational reasoning, but we shall not consider those systems in this note.

2 Results without Computers

Most of the results presented here, although obtained without the use of computers, are easily proved by an equational theorem proving program such as Otter.[3,4]

2.1 Group-like Algebras

In 1938, Tarski presented the following axiom for Abelian group theory in terms of division.[5]

$$(x/(y/(z/(x/y)))) = z \tag{1}$$

In 1952, Higman and Neumann gave the following single axiom for (ordinary) group theory in terms of division.[6]

$$(x/((((x/x)/y)/z)/(((x/x)/x)/z))) = y \tag{2}$$

More generally, Higman and Neumann presented a single axiom *schema* that allows one to construct a single axiom for any subvariety of group theory that can be specified with an equation $\delta = e$, for some term δ.

In 1981, Neumann presented the following axiom for (ordinary) groups in terms of product and inverse.[1]

$$(x \cdot (((y^{-1} \cdot (x^{-1} \cdot z))^{-1} \cdot u) \cdot (y \cdot u)^{-1})^{-1}) = z \tag{3}$$

At the same time, Neumann presented a single axiom schema (analogous to the schema for division) for groups in terms of product and inverse. For example, a single axiom for Abelian groups can be obtained by plugging $(x \cdot y) \cdot (y \cdot x)^{-1}$ into the schema.

In 1969, Padmanabhan presented an axiom for inverse loops in terms of division,[7]

$$(u/u)/((x/y)/(z/(y/x))) = z, \tag{4}$$

along with an axiom schema. The schema generalizes the Higman and Neumann schema for groups in terms of division, because group theory is a subvariety of inverse loops.

In 1968, Meredith and Prior gave the following axiom for Boolean groups, that is, groups in which $x \cdot x = e$.[8]

$$(((y \cdot x) \cdot z) \cdot (y \cdot z)) = x \tag{5}$$

2.2 Lattice-like Algebras

Results on single axioms for lattice-like algebras are less extensive than results for group-like algebras.

In 1973, Padmanabhan and Quackenbush[9] presented a method for constructing a single axiom for any finitely based theory that has particular distributive and permutable congruences. Lattice theory (and therefore Boolean algebra) has these properties. However, straightforward application of the method usually yields single axioms of enormous length. In fact, a simple calculation shows that a straightforward application of the method to Boolean algebra in terms of the Sheffer stroke would produce a single axiom with more than 40 million symbols!

If the construction method is applied to ternary Boolean algebra, that is, Boolean algebra in terms of a ternary operation $f(x, y, z) = xy + yz + zx$, the following axiom[a] is produced.[10]

$$\begin{aligned} f(f(x, x', y), (f(f(z, (f(f(u, v, w), v_6, f(u, v, v_7)))', \\ f(v, f(v_7, v_6, w), u)), v_8', z))', z) = y \end{aligned} \tag{6}$$

3 Computer-aided Results

Results in this section were obtained with assistance from automated deduction systems. Programs such as Otter[3] were used to search for proofs, and programs such as MACE[11] and SEM[12] were used to search for counterexamples. In addition, special-purpose symbolic computation software was written in several cases.

[a] This axiom was found as part of a project that used computers, but we include it here because it is the result of a straightforward application of the Pixley polynomial reduction method.

3.1 Group-like Structures

In 1993, I presented the 4-variable axiom[2]

$$(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u \tag{7}$$

for group theory in terms of product and inverse. To find axiom (7), tens of thousands of candidate identities were constructed (nonexhuastively), and given to the theorem prover Otter to search for proofs of known bases. At about the same time, Kunen presented the 3-variable axiom for the same theory.[13]

$$(((z \cdot (x \cdot y)^{-1})^{-1} \cdot (z \cdot y^{-1})) \cdot (y^{-1} \cdot y)^{-1}) = x \tag{8}$$

More important, Kunen proved that there is no axiom shorter than axiom (7) for group theory in terms of product an inverse by constructing countermodels (by hand and with computers) for all shorter group identities.

In 1993, I gave the axiom

$$(((x \cdot y) \cdot z) \cdot (x \cdot z)^{-1}) = y \tag{9}$$

for Abelian groups in terms of product and inverse,[2] simplifying the results of Neumann.[1]

In 1995, Kunen and I found the schema[14]

$$((\gamma \cdot z)^{-1} \cdot y) \cdot ((\delta \cdot (z \cdot x))^{-1} \cdot y)^{-1} = x \tag{10}$$

for group theory in terms of product and inverse, simplifying and generalizing the Neumann schema[1] In Equation (10), the subvariety is specified by $\gamma = \delta$.

In 1995, for inverse loops, Padmanabhan and I presented the schema[15]

$$x \cdot ((((x \cdot y^{-1}) \cdot y)^{-1} \cdot z) \cdot ((\delta \cdot u)^{-1} \cdot (\gamma \cdot u))) = z \tag{11}$$

and the corresponding axiom

$$x \cdot ((((x \cdot y^{-1}) \cdot y)^{-1} \cdot z) \cdot (u^{-1} \cdot u)) = z \tag{12}$$

The schema 11, although longer than the schema 10, is more general in the sense that groups are a subvariety of inverse loops.

A group of exponent n is a group satisfying $x^n = e$. For example, groups of exponent 2 are the Boolean groups. A shortest single axiom for Boolean groups was already known.[8] In 1992, the Wos and I presented a schema for short axioms for groups of odd exponent.[16] For exponent 3 groups, the schema produces the axiom

$$x \cdot ((x \cdot (x \cdot (y \cdot (z \cdot z)))) \cdot z) = y. \tag{13}$$

In 1995, Kunen presented the axiom[14]

$$(y \cdot ((y \cdot ((y \cdot y) \cdot (x \cdot z))) \cdot (z \cdot (z \cdot z)))) = x \tag{14}$$

for groups of exponent 4 and proved that there is none shorter.

3.2 Lattice-like Structures

In 1995, Padmanabhan and I presented the axiom[10]

$$f(f(x, x', y), (f(f(z, u, v), w, f(z, u, v_6)))', f(u, f(v_6, w, v), z)) = y. \tag{15}$$

for ternary Boolean algebra. It was found using Otter to derive identities from Equation (6), then using Otter again for each identity to search for a proof of a known basis.

In 1996, Padmanabhan and I presented the single axiom[17]

$$\begin{aligned}&(((x \wedge y) \vee (y \wedge (x \vee y))) \wedge z) \vee (((x \wedge (((x_1 \wedge y) \vee (y \wedge x_2)) \vee \\ &\quad y)) \vee (((y \wedge (((x_1 \vee (y \vee x_2)) \wedge (x_3 \vee y)) \wedge y)) \vee (u \wedge (y \vee \\ &\quad (((x_1 \vee (y \vee x_2)) \wedge (x_3 \vee y)) \wedge y)))) \wedge (x \vee (((x_1 \wedge y) \vee (y \wedge \\ &\quad x_2)) \vee y)))) \wedge (((x \wedge y) \vee (y \wedge (x \vee y))) \vee z)) = y\end{aligned} \tag{16}$$

for lattice theory. It was found by optimizing, with various automated reasoning techniques, the Pixley polynomial reduction procedure.[9] In addition, a single axiom schema was presented for subvarieties of weakly associative lattices.[17]

Just this year, a short axiom was found for Boolean algebra in terms of the Sheffer stroke, $x|y = x' + y'$. Stephen Wolfram had sent us a set of identities that were under investigation as being possible single axioms, and we proved two of them to be single axioms, including the following.[18]

$$(x \mid ((y \mid x) \mid x)) \mid (y \mid (z \mid x)) = y \tag{17}$$

The proofs were quite difficult, and several interesting 2-equation bases were found along the way.

Finally, also this year, the following short single axiom was found for Boolean algebra in terms of disjunction and negation.[18]

$$(((x + y)' + z)' + (x + (z' + (z + u)')')')' \;=\; z \tag{18}$$

An extensive and complex search was required to find this axiom (and several others of the same size). The general technique was to

1. Generate well-formed equations under a set of constraints.

2. Apply a truth-table procedure to extract Boolean identities.

3. Build a set of finite non-Boolean algebras. These were found by applying the model-searching programs MACE[11] and SEM[12] to search for non-Boolean (e.g., noncommutative or nonidempotent) models of candidate identities. The non-Boolean algebras have up to eight elements.

4. Eliminate candidates that are true in any of the non-Boolean algebras.

Acknowledgments

I have worked with many on these problems, including R. Padmanabhan, Larry Wos, Bob Veroff, Rusty Lusk, Branden Fitelson, Kenneth Harris, Andrew Feist, and Ken Kunen.

This work was supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

References

1. B. H. Neumann. Another single law for groups. *Bull. Australian Math. Soc.*, 23:81–102, 1981.
2. W. McCune. Single axioms for groups and Abelian groups with various operations. *J. Automated Reasoning*, 10(1):1–13, 1993.
3. W. McCune. Otter 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL, 1994.
4. W. McCune. Otter. `http://www.mcs.anl.gov/AR/otter/`, 1994.
5. A. Tarski. Ein Beitrag zur Axiomatik der Abelschen Gruppen. *Fundamenta Mathematicae*, 30:253–256, 1938.
6. G. Higman and B. H. Neumann. Groups as groupoids with one law. *Publicationes Mathematicae Debrecen*, 2:215–227, 1952.
7. R. Padmanabhan. Inverse loops as groupoids with one law. *J. London Math. Soc.*, 2(1 44):203–206, 1969.
8. C. A. Meredith and A. N. Prior. Equational logic. *Notre Dame J. Formal Logic*, 9:212–226, 1968.
9. R. Padmanabhan and R. W. Quackenbush. Equational theories of algebras with distributive congruences. *Proc. of AMS*, 41(2):373–377, 1973.
10. R. Padmanabhan and W. McCune. Single identities for ternary Boolean algebras. *Computers and Mathematics with Applications*, 29(2):13–16, 1995.

11. W. McCune. MACE: Models and Counterexamples. `http://www.mcs.anl.gov/AR/mace/`, 1994.
12. J. Zhang and H. Zhang. SEM: A system for enumerating models. In *Proceedings of the International Joint Conference on Artificial Intelligence*, 1995.
13. K. Kunen. Single axioms for groups. *J. Automated Reasoning*, 9(3):291–308, 1992.
14. K. Kunen. The shortest single axioms for groups of exponent 4. *Computers and Mathematics with Applications*, 29:1–12, 1995.
15. W. McCune and R. Padmanabhan. *Automated Deduction in Equational Logic and Cubic Curves*, volume 1095 of *Lecture Notes in Computer Science (AI subseries)*. Springer-Verlag, Berlin, 1996.
16. W. McCune and L. Wos. Application of automated deduction to the search for single axioms for exponent groups. In A. Voronkov, editor, *Logic Programming and Automated Reasoning, LNAI Vol. 624*, pages 131–136, Berlin, 1992. Springer-Verlag.
17. W. McCune and R. Padmanabhan. Single identities for lattice theory and weakly associative lattices. *Algebra Universalis*, 36(4):436–449, 1996.
18. W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos. Single axioms for Boolean algebra. Preprint ANL/MCS-P848-1000, Argonne National Laboratory, Argonne, IL, 2000.