Algebra univers. **52** (2004) 541–549
0002-5240/04/040541 – 09
DOI 10.1007/s00012-004-1902-0

Algebra Universalis

Automated discovery of single axioms for ortholattices

W. McCune, R. Padmanabhan, M. A. Rose, and R. Veroff

Abstract. We present short single axioms for ortholattices, orthomodular lattices, and modular ortholattices, all in terms of the Sheffer stroke. The ortholattice axiom is the shortest possible. We also give multiequation bases in terms of the Sheffer stroke and in terms of join, meet, and complementation. Proofs are omitted but are available in an associated technical report and on the Web. We used computers extensively to find candidates, reject candidates, and search for proofs that candidates are single axioms.

1. Introduction

Consider the problem of expressing equational theories as simply as possible — with the least number of symbols, the least number of equations, the least number of operations, and the least number of variables. The problem for Abelian groups was solved by Tarski in 1938 [15] with the single axiom $x/(y/(z/(x/y))) = z$ in terms of the division operation. Other varieties of groups (including other operations) have been addressed, and short single axioms have been found, but minimality has not been proved in most cases.

The problem for Boolean algebras was solved recently with a shortest single axiom in terms of the Sheffer stroke operation [10]. Progress has recently been made also for lattices, with a reasonably short single axiom in terms of join and meet [9]. In this paper we consider a chain of varieties between lattices and Boolean algebras, namely, ortholattices, orthomodular lattices, and modular ortholattices.

The main results of the work we report here are all in terms of the Sheffer stroke — a shortest single axiom for ortholattices, and short single axioms for orthomodular lattices and modular ortholattices. We also include multiequation bases for these varieties.

Presented by G. Grätzer.
Received February 26, 2004; accepted in final form September 14, 2004.
2000 *Mathematics Subject Classification*: 03G10; 06B99.
Key words and phrases: Ortholattice basis, ortholattice single identity.
The first author was supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, Office of Science, U.S. Department of Energy, under Contract W-31-109-ENG-38. The second author was supported by an operating grant from NSERC of Canada, grant #8215-02. The third author was supported by the Division of Educational Programs, Argonne National Laboratory. The fourth author was supported by National Science Foundation grant CDA-9503064.

We used several computer programs in this work. Otter [5] searches for proofs, Mace [4] searches for models and counterexamples, and other programs embody decision and enumeration procedures. We claim, throughout the paper, that Otter proves theorems and that Mace finds counterexamples. We have omitted the proofs and counterexamples because they are long and because they do not seem to give insight into the mathematics. The proofs and counterexamples can be found in a technical report [7] and on a Web page [8]. The Web page contains, in addition, input and output files for Otter and Mace and demonstrations of the enumeration, decision, and filtering programs that were used.

2. Multiequation bases

We define the relevant varieties first in terms of join, meet, and complementation and then in terms of the Sheffer stroke.

2.1. In terms of join/meet/complementation. Consider the following equations.

$$\begin{aligned}
\text{(AJ):}\quad & x \vee (y \vee z) = y \vee (x \vee z) \\
\text{(AM):}\quad & x \wedge (y \wedge z) = y \wedge (x \wedge z) \\
\text{(B1):}\quad & x \vee (x \wedge y) = x \\
\text{(B2):}\quad & x \wedge (x \vee y) = x \\
\text{(DM):}\quad & x \wedge y = (x' \vee y')' \\
\text{(CC):}\quad & x'' = x \\
\text{(ONE):}\quad & x \vee x' = y \vee y' \\
\text{(OM):}\quad & x \vee (x' \wedge (x \vee y)) = x \vee y \\
\text{(MOD):}\quad & x \vee (y \wedge (x \vee z)) = x \vee (z \wedge (x \vee y)) \\
\text{(CUT):}\quad & (x \vee y') \wedge (x \vee y) = x
\end{aligned}$$

The lattices ($\mathcal{L}$), ortholattices ($\mathcal{OL}$), orthomodular lattices ($\mathcal{OML}$), modular ortholattices ($\mathcal{MOL}$), and Boolean algebras ($\mathcal{BA}$) can be defined as shown in the following table.

Variety	Type	Basis
$\mathcal{L}$	$\langle 2,2 \rangle$	{ (AJ), (B1), (AM), (B2) }
$\mathcal{OL}$	$\langle 2,2,1 \rangle$	{ (AJ), (B1), (DM), (CC), (ONE) }
$\mathcal{OML}$	$\langle 2,2,1 \rangle$	{ (AJ), (B1), (DM), (OM) }
$\mathcal{MOL}$	$\langle 2,2,1 \rangle$	{ (AJ), (B1), (DM), (CC), (ONE), (MOD) }
$\mathcal{BA}$	$\langle 2,2,1 \rangle$	{ (AJ), (DM), (ONE), (CUT) }

Otter can easily prove that these bases are equivalent to other bases given in the literature (for example, by deriving the commutativity laws from the $\mathcal{L}$ basis),

Mace can easily show that all but the $\mathcal{BA}$ basis are independent (we do not know if (ONE) is necessary), Otter can easily show that these varieties form the chain

$$\mathcal{L} \supset \mathcal{OL} \supset \mathcal{OML} \supset \mathcal{MOL} \supset \mathcal{BA},$$

and Mace can easily show that those inclusions are proper.

2.2. In terms of the sheffer stroke. The lattices cannot be defined in terms of a single binary operation [2], but $\mathcal{OL}$ and its subvarieties can be, in particular, in terms of the Sheffer stroke "|".

	terms of $\vee, \wedge, '$	$\vee, \wedge, '$ in terms of $\mid$
$x \mid y = x' \vee y'$		$x \vee y = (x \mid x) \mid (y \mid y)$
		$x \wedge y = (x \mid y) \mid (x \mid y)$
		$x' = x \mid x$

Rewriting a basis to a different set of operations does not necessarily produce a basis in terms of that other set of operations. If we use the definitions just given to rewrite a Sheffer stroke basis in terms of join and complementation, we do not get a basis in terms of join and complementation. This statement applies to $\mathcal{OL}$, $\mathcal{OML}$, $\mathcal{MOL}$, and $\mathcal{BA}$, and it is independent of the basis we start with. Consider (BA2), a single axiom for $\mathcal{BA}$ [10]. Construct candidate (BA2′) from (BA2) by replacing $x \mid y$ with $x' \vee y'$ throughout as follows (the spacing shows the correspondence).

$$\begin{array}{lll} (\,y\ \mid (\,(\,x\ \mid\ y\ )\ \mid\ y\ )\ )\ \mid (\,x\ \mid (\,z\ \mid\ y\ )\ )\ = x & & \text{(BA2)} \\ (\,y' \vee (\,(\,x' \vee y'\,)' \vee y'\,)'\,)' \vee (\,x' \vee (\,z' \vee y'\,)'\,)' = x & & \text{(BA2}') \end{array}$$

If (BA2′) were a single axiom, we would be able to derive associativity of join, but this is impossible: if we interpret x' as x, (BA2′) becomes identical to (BA2) except for the operation symbol; hence the models of (BA2), in which the Sheffer stroke is nonassociative, immediately give models of (BA2′) in which join is nonassociative.

Considering the other direction, if we rewrite a join/meet/complementation basis in terms of the Sheffer stroke, we do obtain a basis in terms of the Sheffer stroke (the proof is omitted). However, this translation can produce equations more complicated than necessary; for example, equation AJ rewritten to the Sheffer stroke is

$$(x|x)|(((y|y)|(z|z))|((y|y)|(z|z))) = (y|y)|(((x|x)|(z|z))|((x|x)|(z|z))).$$

However, because the Sheffer stroke operation builds in properties of complementation, we can find simpler bases with Sheffer stroke than with join, meet, and complementation.

Consider the following equations.

$$\begin{array}{ll}
(\widehat{\mathrm{A}}): & x \,|\, ((y \,|\, z) \,|\, (y \,|\, z)) = y \,|\, ((x \,|\, z) \,|\, (x \,|\, z)) \\
(\widehat{\mathrm{B}}): & (x \,|\, x) \,|\, (x \,|\, y) = x \\
(\widehat{\mathrm{ONE}}): & x \,|\, (x \,|\, x) = y \,|\, (y \,|\, y) \\
(\widehat{\mathrm{OM}}): & x \,|\, (x \,|\, (x \,|\, y)) = x \,|\, y \\
(\widehat{\mathrm{MOD}}): & x \,|\, (y \,|\, (x \,|\, (z \,|\, z))) = x \,|\, (z \,|\, (x \,|\, (y \,|\, y))) \\
(\widehat{\mathrm{CUT}}): & (x \,|\, (y \,|\, y)) \,|\, (x \,|\, y) = x
\end{array}$$

The varieties in question can be defined as shown in the following table.

Variety	Type	Basis
$\mathcal{OL}$	$\langle 2 \rangle$	{ $\widehat{\mathrm{A}}$, $\widehat{\mathrm{B}}$, $\widehat{\mathrm{ONE}}$ }
$\mathcal{OML}$	$\langle 2 \rangle$	{ $\widehat{\mathrm{A}}$, $\widehat{\mathrm{B}}$, $\widehat{\mathrm{OM}}$ }
$\mathcal{MOL}$	$\langle 2 \rangle$	{ $\widehat{\mathrm{A}}$, $\widehat{\mathrm{B}}$, $\widehat{\mathrm{ONE}}$, $\widehat{\mathrm{MOD}}$ }
$\mathcal{BA}$	$\langle 2 \rangle$	{ $\widehat{\mathrm{A}}$, $\widehat{\mathrm{CUT}}$ }

Mace easily shows that these bases are independent, and Otter easily proves that these bases are definitionally equivalent to the join/meet/complementation bases in the preceding subsection.

2.3. Do simpler multiequation bases exist? Our goal in producing the multiequation bases was to find short, intuitive, and fairly standard bases in terms of join/meet/complementation and then to find similar bases in terms of the Sheffer stroke. We doubt that the preceding bases are the shortest. In fact, for $\mathcal{BA}$ in terms of the Sheffer stroke, the 2-basis with the least number of symbols is known to be { $x \,|\, y = y \,|\, x$, $(x \,|\, y) \,|\, (x \,|\, (y \,|\, z)) = x$ } [17]. For $\mathcal{BA}$ in terms of the join and complementation, the simplest 2-basis we know of is { $(x' \vee y)' \vee x = x$, $(x' \vee y)' \vee (z \vee y) = y \vee (z \vee x)$ } [11].

3. Single axioms

It is well known that any finitely-based variety of $\mathcal{OML}$ is one-based [13]. This is a consequence of the existence of Gould-Grätzer-Pixley (GGP) terms [1, 14] in these varieties; that is, terms $g(x, y, z)$ such that $g(y, y, x) = g(x, z, z) = g(x, u, x) = x$. For example, $(x \wedge z) \vee ((y \wedge z)' \wedge z) \vee ((x \wedge y)' \wedge x)$ is a GGP term for $\mathcal{OML}$.

The variety $\mathcal{OL}$ does not admit GGP terms, and existence of single axioms is known by a different result [12], relying on a basis consisting entirely of absorption equations and the presence of majority terms; that is, terms $m(x, y, z)$ such that $m(x, x, y) = m(x, z, x) = m(u, x, x) = x$.

By those results, there exist procedures to construct single axioms for these varieties, but the basic procedures have exponential behavior, producing very large

axioms, sometimes with millions of symbols. The procedures can be optimized somewhat [6], but they still tend to produce axioms with hundreds of symbols.

Our approach is to start small, considering all possible candidate equations of a given size, and looking at sizes as large as practical. If all goes well, we can show that a candidate is a shortest single axiom by proving a known basis and by eliminating all shorter candidates. In other cases, we can find single axioms without being able to eliminate all shorter candidates.

A similar approach led, in previous work, to axiom (LT1) (below) for lattice theory [9], axiom (BA1) for Boolean algebra [10], and (BA2), which is a shortest axiom for Boolean algebra in terms of the Sheffer stroke [10].

$$\text{(LT1):}\quad (((y \vee x) \wedge x) \vee (((z \wedge (x \vee x)) \vee (u \wedge x)) \wedge v)) \wedge (w \vee ((s \vee x) \wedge (x \vee t))) = x$$
$$\text{(BA1):}\quad ((y \vee z)' \vee x')' \vee ((u' \vee u)' \vee (x' \vee y))' = x$$
$$\text{(BA2):}\quad (y \mid ((x \mid y) \mid y)) \mid (x \mid (z \mid y)) = x$$

Our goal in this work was to find short single axioms for $\mathcal{OL}$, $\mathcal{OML}$, and $\mathcal{MOL}$ in terms of the Sheffer stroke.

3.1. Generating and filtering candidates. The procedure to generate candidates equations is roughly as follows.

- Generate all well-formed Sheffer stroke equations of a given length satisfying the following constraints: (1) it has at least three variables; (2) its right-hand side is a variable, say x; (3) neither the leftmost nor the rightmost variable of the left-hand side is x; (4) it cannot be of the form $y|\alpha = x$ or $\alpha|y = x$ for any variable y; and (5) if it is $\alpha|\beta = x$, then length$(\alpha) \leq$ length(β). Justifications for these constraints can be found in [10].
- Pass the equations through a decision procedure for Boolean algebra identities. A vast majority of the equations are removed by this check.
- Remove equations that are not valid in the variety in question. For $\mathcal{OL}$ we have a decision procedure for this. For $\mathcal{OML}$ and $\mathcal{MOL}$, for which there is no decision procedure [3, p. 218], we can test the equations against a set of finite models of the variety (perhaps admitting some nonidentities).
- Eliminate candidates that are too weak to be single axioms. We do not have a perfect test for this. In practice, we iteratively collect sets of nonmodels by using the program Mace. Consider $\mathcal{OL}$. If a candidate is false in all of the current non-$\mathcal{OL}$s, we use Mace to look for non-$\mathcal{OL}$ models of the candidate. If one is found, we add it to the set and eliminate the candidate. We call this process *filtering the candidates*, and we refer to the nonmodels as *filters*.

Let the *length* of a term or equation be the number of occurrences of variables and operators (including the equal sign but not parentheses). For example, $(x \mid x) \mid (x \mid y) = x$ has length 9. Note that Sheffer stroke equations have odd length.

In the $\mathcal{OL}$ case, all candidates up through length 21 can be eliminated by a set of four non-$\mathcal{OL}$s [8, file non-OL.A-4] of sizes 3, 6, 6, and 8. A single axiom ((OL-Sh) below) was found among the candidates of length 23.

In the $\mathcal{OML}$ case, all candidates up through length 19 can be eliminated with a set of nine non-$\mathcal{OL}$s [8, file non-OL.B-9], all of size ≤ 6. For length 21, we could not eliminate all candidates, and we could not prove any of the survivors to be single axioms. A set of 23 non-$\mathcal{OL}$s was accumulated [8, file non-OL.C-23], eliminating all but 58 candidates. A single axiom ((OML-Sh) below) was found among the candidates of length 23.

The $\mathcal{MOL}$ case started out like the $\mathcal{OML}$ case, with the elimination of all candidates up through length 19 by using the same filters as in the $\mathcal{OML}$ case. For length 21, 14 more non-$\mathcal{OL}$s were accumulated [8, file non-OL.D-14], and the nine nonmodular $\mathcal{OML}$s up through size 16 were also used as filters. However, 238 length 21 candidates survived, and none was proved to be a single axiom. As the candidates grow, it becomes more difficult to find counterexamples, so we used the existing non-$\mathcal{MOL}$s to filter candidates of lengths 23, 25, and 27. A single axiom ((MOL-Sh) below) was found among those of length 25.

3.2. An example candidate and counterexample. One of the $\mathcal{OML}$ candidates was the identity

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

Given this candidate, with no additional constraints, Mace could not find a counterexample in a reasonable amount of time. However, when asked Mace to search for a quasigroup model of (C), it immediately found the following structure.

	0	1	2	3	4	5	6
0	0	2	1	4	3	6	5
1	3	5	4	0	2	1	6
2	4	3	6	1	0	5	2
3	5	1	3	2	6	0	4
4	6	4	2	5	1	3	0
5	2	6	0	3	5	4	1
6	1	0	5	6	4	2	3

It is easy to see that this structure is not an ortholattice with respect to the Sheffer stroke (e.g., because it contains an idempotent element, or because it is noncommutative, or simply because it is a quasigroup). Hence, (C) cannot be a single axiom for any subvariety of $\mathcal{OL}$. This structure became a member of the filter set non-OL.C-23 listed in [8].

3.3. Trying to prove that candidates are single axioms. Given a set of candidates that had survived all the filters, we tried to prove each to be a single axiom by deriving a known basis, for example, the independent bases given in Section 2.

Automatic proofs were attempted with hundreds of $\mathcal{OL}$ candidates, thousands of $\mathcal{OML}$ candidates, and hundreds of thousands of $\mathcal{MOL}$ candidates before proofs were found for the three cases. The time allocated for each candidate varied from a few minutes to a few seconds, depending on the size of the set. For each proof attempt, we included as goals several important properties of the variety as well as a known basis. If some interesting properties were derived from the candidate, but not enough for a complete proof, we investigated that candidate later with focused proof attempts.

Length 23 single axioms for $\mathcal{OL}$ and $\mathcal{OML}$ were found without much difficulty. The proofs were not trivial for Otter, but they were found automatically within a few minutes. Finding a $\mathcal{MOL}$ axiom was much more difficult. Many more candidates had to be considered, and proofs with the successful candidates were not found automatically. Promising candidates (those that proved the most interesting properties) were selected from the automatic attempts, and advanced automated deduction techniques involving human guidance (i.e., the method of hints and sketches [16]) were applied, producing a proof for one candidate of length 25.

3.4. Single axioms for $\mathcal{OL}$, $\mathcal{OML}$, and $\mathcal{MOL}$. We give here the main results of the project — single axioms, in terms of the Sheffer stroke, for $\mathcal{OL}$, $\mathcal{OML}$, and $\mathcal{MOL}$. Proofs can be found in [7] and in [8]. For completeness, we also list (BA2), a shortest single axiom for $\mathcal{BA}$ [10].

$$\begin{aligned}
\text{(OL-Sh):}\quad & (((y \mid x) \mid (x \mid z)) \mid u) \mid (x \mid ((x \mid ((y \mid y) \mid y)) \mid z)) = x \\
\text{(OML-Sh):}\quad & (((y \mid x) \mid (x \mid z)) \mid u) \mid (x \mid ((z \mid ((x \mid x) \mid z)) \mid z)) = x \\
\text{(MOL-Sh):}\quad & (y \mid x) \mid (((x \mid x) \mid z) \mid (((((x \mid y) \mid z) \mid z) \mid x) \mid (x \mid u))) = x \\
\text{(BA2):}\quad & (y \mid ((x \mid y) \mid y)) \mid (x \mid (z \mid y)) = x
\end{aligned}$$

The $\mathcal{OL}$ axiom (length 23) is the shortest possible. We do not know whether the $\mathcal{OML}$ axiom (length 23) or the $\mathcal{MOL}$ axiom (length 25) are shortest.

With the exception of (BA2), each of these axioms has four variables, and the question of short 3-variable axioms is open. In the $\mathcal{OL}$ case, all of the surviving length-23 candidates have 4 variables, so any 3-variable $\mathcal{OL}$ axioms must have length ≥ 25. In the $\mathcal{OML}$ case, four of the 58 length-21 and many of the length-23 candidates have three variables. In the $\mathcal{MOL}$ case, many of the surviving candidates of lengths 21 and 23 have three variables.

4. Conclusion

Symbolic computation was used in five ways in this work: (1) to enumerate equations subject to a set of syntactic constraints, (2) to evaluate equations with respect to finite structures, (3) to decide ortholattice identities, (4) to search (with Otter) for equational proofs, and (5) to search (with Mace) for finite algebras that satisfy sets of equations and disequations. The first three ways are relatively straightforward, although the programs were coded efficiently so that they could handle billions of equations. Otter and Mace are available for download from the Web page associated with this paper [8].

The proofs in this work fall into several classes: proofs by equational deduction, independence proofs by finite counterexamples, and minimality proofs by exhaustive enumeration.

The minimality proofs are fundamentally different from the Otter or Mace proofs and are similar in spirit (though not in scale or interest) to proofs of the four-color theorem. In short, the problem is reduced to a finite set of cases that are checked by computers. Soundness is especially questionable, with reliance (in our case) on optimized special-purpose code for the equation generation and decision procedures. We doubt that much can be learned from the various components of the minimality proofs.

The Otter proofs and Mace counterexamples, on the other hand, are creative in the sense that we had no idea what the proofs or structures might be and the proofs, with the exception of the $\mathcal{MOL}$ single axiom proof, required little human guidance.

References

[1] M. I. Gould and G. Grätzer, *Boolean extensions and normal subdirect powers of finite universal algebras*, Math. Zeitschr. **99** (1967), 16–25.
[2] G. Grätzer, *General Lattice Theory*, 2nd edition, Birkhauser Verlag, 1998.
[3] G. Kalmbach, *Orthomodular Lattices*, Academic Press, New York, 1983.
[4] W. McCune, *Mace4 Reference Manual and Guide*, Tech. Memo ANL/MCS-TM-264, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, August 2003.
[5] W. McCune, *Otter 3.3 Reference Manual*, Tech. Memo ANL/MCS-TM-263, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, August 2003.
[6] W. McCune and R. Padmanabhan, *Single identities for lattice theory and for weakly associative lattices*, Algebra Universalis **36** (1996), 436–449.
[7] W. McCune, R. Padmanabhan, M. A. Rose, and R. Veroff, *Short equational bases for ortholattices: Proofs and countermodels*, Tech. Memo ANL/MCS-TM-265, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, September 2003.
[8] W. McCune, R. Padmanabhan, M. A. Rose, and R. Veroff, *Short equational bases for ortholattices: Web support*, `http://www.mcs.anl.gov/~mccune/papers/olsax/`, 2003.

[9] W. McCune, R. Padmanabhan, and R. Veroff, *Yet another single law for lattices*, Algebra Universalis, to appear.
[10] W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos, *Short single axioms for Boolean algebra*, J. Automated Reasoning **29** (2002), 1–16.
[11] C. A. Meredith and A. N. Prior, *Equational logic*, Notre Dame J. Formal Logic **9** (1968), 212–226.
[12] R. Padmanabhan, *Equational theory of algebras with a majority polynomial*, Algebra Universalis **7** (1977), 273–275.
[13] R. Padmanabhan and R. W. Quackenbush, *Equational theories of algebras with distributive congruences*, Proc. AMS **41** (1973), 373–377.
[14] A. F. Pixley, *The ternary discriminator function in universal algebra*, Math. Ann. **191** (1971), 167–180.
[15] A. Tarski, *Ein Beitrag zur Axiomatik der Abelschen Gruppen*, Fundamenta Mathematicae **30** (1938), 253–256.
[16] R. Veroff, *Solving open questions and other challenge problems using proof sketches*, J. Automated Reasoning **27** (2001), 157–174.
[17] R. Veroff, *A shortest 2-basis for Boolean algebra in terms of the Sheffer stroke*, J. Automated Reasoning **31** (2003), 1–9.

W. McCune
Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL 60439, USA
e-mail: mccune@mcs.anl.gov

R. Padmanabhan
Department of Mathematics, University of Manitoba, Winnipeg R3T 2N2, Canada
e-mail: padman@cc.umanitoba.ca

M. A. Rose
Department of Mathematics, University of Wisconsin-Madison, Madison, WI 53706, USA
e-mail: rose@math.wisc.edu

R. Veroff
Department of Computer Science, University of New Mexico, Albuquerque, New Mexico 87131, USA
e-mail: veroff@cs.unm.edu