Preprint MCS-P386-1093, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, Ill., November 1993.

Single Identities for Ternary Boolean Algebras

R. Padmanabhan[*]
Department of Mathematics
University of Manitoba
Winnipeg, Manitoba R3T 2N2
Canada

W. McCune[†]
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4844
U.S.A.

1 Introduction

Ternary Boolean algebras (TBA) are algebras of type $\langle 3,1\rangle$ with one ternary operation f and one unary operation g defined by $f(x,y,z) = xy + yz + zx$ and $g(x) = x'$, where "+", ".", and "′" are the Boolean join, meet and complementation operations. These operations were originally studied by A. A. Grau [2]. By the equational theory of TBAs we mean the study of the set of all equational identities satisfied by f and g in all Boolean algebras. In this paper, we show that the equational theory of TBAs is one-based.

Our methods for finding a single identity for the theory of TBAs are interesting from two distinct points of view. First, from the algebraic, since TBAs enjoy both permutable and distributive congruences, they admit a single ternary polynomial $p(x,y,z)$, the so-called Pixley polynomial [1, p. 405]. We first find such a polynomial $p(x,y,z)$ and use a technique of R. Padmanabhan and R. W. Quackenbush [7] to construct a single identity for the equational theory in question. This is done in Section 2. Second, from the viewpoint of automated reasoning, we use the program OTTER to discover new single identities based upon the results of the algebraic view. Actually we obtain here three new identities—shorter in length than those obtained by the formal algebraic process of Section 2—each characterizing the equational theory of TBAs. The relevant OTTER proofs are also included.

2 The Algebraic View

LEMMA 1. *The following three identities characterize TBAs:*

$$(1) \qquad f(f(a,b,c),d,f(a,b,e)) = f(b,f(e,d,c),a),$$

$$(2) \qquad f(x,g(y),x) = x,$$

$$(3) \qquad f(x,g(x),y) = y.$$

[*] Supported by an operating grant from NSERC of Canada (#A8215).

[†] Supported by the Office of Scientific Computing, U.S. Department of Energy, under Contract W-31-109-Eng-38.

Proof. Substitute $e = c$ in (1) and say, $d = g(u)$, and use (2) to get

$$(4) \qquad f(a,b,c) = f(b,c,a) = f(c,a,b).$$

Substitute $b = g(a)$ in (1), and use (3) and (4) to get $f(c,d,e) = f(e,d,c)$. Thus the ternary f has now all six symmetries. Finally, we show that $g(g(y)) = y$. Let $x = g(y)$ in (3). We have $y = f(g(y), g(g(y)), y) = f(y, g(y), g(g(y))) = g(g(y))$. Thus, by A. A. Grau [2], we have obtained all the necessary identities for TBAs.

Let (5) be the dual of (3), namely,

$$(5) \qquad f(x, g(y), y) = x,$$

which, of course, is a consequence of $\{(1), (2), (3)\}$. The identities (2), (3) and (5) give the two-thirds minority and one-third majority property for the composite ternary polynomial $p(x,y,z) := f(x, g(y), z)$, that is,

$$p(x,x,z) = p(z,y,y) = p(z,y,z) = z.$$

Thus, TBAs form a finitely based equational class of algebras of type $\langle 3, 1\rangle$—with one ternary and one unary—defined by (i) $s(a,b,c,d,e) = t(a,b,c,d,e)$, written in the language of f and g (actually only f), and (ii) the composite ternary being a two-thirds minority and one-third majority polynomial, again in the language of type $\langle 3, 1\rangle$ using f and g. Hence, by Padmanabhan and Quackenbush [7], there exists a single identity of the same type (i.e., in the language of f and g) equivalent to the four identities that characterize the TBAs. To write such an identity, we simply follow the technique given in [7, p. 376]; the identity (8) of Theorem 2 of that paper is the desired one:

$$(6) \qquad p(p(u,u,x), p(w,y,z), z) = x,$$

where the word $w(z,a,b,c,d,e) = p(z, s(a,b,c,d,e), t(a,b,c,d,e))$. Let us now write the identity in full:

$$(7) \qquad f(f(x,g(x),y), g(f(f(z,g(f(f(u,v,w),v6,f(u,v,v7))),f(v,f(v7,v6,w),u)),g(v8),z)),z) = y.$$

This completes the proof of the following theorem.

Theorem 1. *The equational theory of TBAs is one-based.*

3 Searching for a Simpler Single Axiom for TBAs

Otter [4, 5] is a computer program that can be used to search for proofs of statements in first-order logic with equality. Some of the Otter methods presented in [6] were used to search for new single identities simpler than (7). First, we used Otter to generate approximately one thousand TBA identities, using (7) as the initial identity. We constrained each identity to have fewer than 41 symbols. (Symbol count includes f, g, $=$, and variables; e.g., (2) has symbol count 7). Demodulation (simplification) was not used while generating the identities.

Then, with each of the candidate identities, we ran a separate Otter search, trying to prove it to be a single identity. The strategy for these Otter searches was the following:

use a search based on the Knuth-Bendix completion procedure [3]; discard equalities with more than 40 symbols; use (1), (2), and (3) as goals; and search for 60 seconds.

Two of the candidates, one with 26 symbols and the other with 38 symbols, derived all three goals. (7) has 34 symbols.

We now present a proof that the 26-symbol equation is a single identity. The machine-generated derivation below is not the exact proof found by OTTER. It is the result of some special techniques to coerce the program into finding shorter, more presentable proofs. It was, however, generated by computer, and only minor editing has been applied. All of the variables are universally quantified. The justification "$m \rightarrow n$" indicates paramodulation from line m into line n, and "$: m, n, \ldots$" indicates demodulation (simplification) with $m, n, \ldots$.

THEOREM 2. *The following equality is a single identity for TBA.*

(8) $\quad f(f(x,g(x),y),g(f(f(z,u,v),w,f(z,u,v6))),f(u,f(v6,w,v),z)) = y.$

Proof. To see that (8) holds in TBA, simplify it to $y = y$ by applying (3), (1), and then $f(x,g(y),y) = x$. To see that {(1),(2),(3)} can be derived from (8), consider the following derivation (which was constructed by OTTER).

4 $\quad f(f(x,g(x),y),g(f(f(z,u,v),w,f(z,u,v6))),f(u,f(v6,w,v),z)) = y$ [(8)]

5 $\quad f(f(x,y,z),g(f(f(u,v,w),v6,f(u,v,v7))),f(v,f(v7,v6,w),u)) =$
$\qquad f(y,f(z,g(f(x,y,v8)),v8),x)$ [4→4]

7 $\quad f(f(x,f(f(y,z,u),g(f(f(y,z,v),x,w)),w),f(y,z,v)),g(f(f(v6,v7,v8),v9,$
$\qquad f(v6,v7,v10))),f(v7,f(v10,v9,v8),v6)) = f(z,f(u,x,v),y)$ [5→4]

9 $\quad f(g(x),f(y,g(f(x,g(x),z)),z),x) = y$ [5→4]

10 $\quad f(f(x,g(x),y),g(f(z,u,f(g(v),f(z,g(f(v,g(v),w)),w),v6))),f(f(z,$
$\qquad g(f(v,g(v),w)),w),f(v6,u,v),g(v))) = y$ [9→4]

12 $\quad f(f(x,g(x),y),g(f(f(z,u,v),f(w,g(f(v,g(v),v6)),v6),f(z,u,g(v)))),f(u,w,z)) = y$ [9→4]

18 $\quad f(f(x,y,z),g(f(f(u,g(u),v),g(f(u,g(u),v)),f(u,g(u),w))),w) =$
$\qquad f(y,f(z,g(f(x,y,v6)),v6),x)$ [9→5]

25 $\quad f(f(x,g(x),y),g(f(z,u,z)),f(f(z,g(f(v,g(v),w)),w),f(v,u,v),g(v))) = y$ [9→10]

29 $\quad f(f(x,y,z),g(f(u,v,u)),f(f(u,g(f(w,g(w),v6)),v6),f(w,v,w),g(w))) =$
$\qquad f(y,f(z,g(f(x,y,v7)),v7),x)$ [4→25]

34 $\quad f(f(x,g(x),y),g(z),f(g(u),f(v,g(f(f(v,u,w),f(g(u),g(f(w,g(w),v6)),v6),$
$\qquad f(v,u,g(w))))),z),u)) = y$ [12→4]

49 $\quad f(f(x,f(y,g(f(y,x,z)),z),y),g(f(f(u,v,w),v6,f(u,v,v7))),f(v,f(v7,v6,w),u)) =$
$\qquad f(f(y,g(f(v8,g(v8),v9)),v9),f(v8,x,v8),g(v8))$ [29→4]

51 $\quad f(f(x,g(x),y),g(f(z,g(z),f(u,g(u),v))),f(g(z),v,z)) = y$ [4→34:9]

54 $\quad f(g(x),y,x) = y$ [51→51:51]

55 $\quad f(x,g(f(y,g(y),z)),z) = x$ [9:54]

63 $\quad f(f(x,g(x),y),g(f(z,g(z),f(u,g(u),v))),v) = y$ [51:54]

86 $\quad f(f(x,f(y,g(f(y,x,z)),z),y),g(f(f(u,v,w),v6,f(u,v,v7))),f(v,f(v7,v6,w),u)) =$
$\qquad f(y,f(v8,x,v8),g(v8))$ [49:55]

88 $\quad g(f(x,g(x),y)) = g(y)$ [55→54]

89 $\quad f(f(x,y,z),g(f(f(u,g(u),v),g(v),f(u,g(u),w))),w) = f(y,f(z,g(f(x,y,v6)),v6),x)$ [18:88]

97 $\quad f(x,g(y),y) = x$ [55:88]

100 $\quad f(x,g(x),y) = y$ [63:88,88,97]

105 $\quad f(x,g(f(f(y,z,u),v,f(y,z,w))),f(z,f(w,v,u),y)) = x$ [4:100]

117 $\quad f(x,f(y,g(f(z,x,u)),u),z) = f(z,x,y)$ [89:100,100,100,97]

120 $\quad f(f(x,y,z),u,f(x,y,v)) = f(y,f(v,u,z),x)$ [7:117,105]

121 $\quad f(x,f(y,z,y),g(y)) = f(x,z,x)$ [86:117,120,97]

123 $g(g(x)) = x$ [100→54]
125 $f(x, y, g(y)) = x$ [123→97]
131 $f(x, g(y), x) = x$ [97→121:125]

Line 100 is (3), line 120 is (1), and line 131 is (2).

We then made a second attempt to find short single identities by simply considering 4642 additional candidates. Forty of the candidates were shown to be single identities; none of those is shorter than (8), and the following two are the same length as (8).

$$f(f(x, g(x), y), g(f(z, f(u, v, w), v6)), f(f(v6, z, w), v, f(v6, z, u))) = y$$
$$f(f(x, g(x), y), g(f(z, f(u, v, w), v6)), f(f(v6, z, u), v, f(v6, z, w))) = y$$

Note. Recall that all of the candidates were derived from (7). Without knowledge of (7), it would have been much more difficult to find short single identities. We made a third attempt to find single identities, this time generating a set of candidates from {(1),(2),(3)}. A set of 555 candidates, all with lengths 20–30, was considered, but none of them was shown to be a single identity.

4 Concluding Remarks

The single identity (8) discovered by OTTER with 26 symbols and 7 variables (along with its equivalent cousins) is the shortest identity we know for defining Boolean algebras under any treatment. We leave open the question of whether there exist single identities with fewer symbols or variables. The only other known treatment of Boolean algebras for which a single identity is known to exist is the famous Sheffer's stroke operation of binary rejection (i.e., *nor*), $x|y = x' \wedge y'$. Here, we have $g(y) = y|y$, $x \wedge y = (x|x)|(y|y)$, and $x \vee y = (x|y)|(x|y)$. Thus, one can once again build the Pixley polynomial $p(x, y, z)$ and hence, by Theorem 1, the equational theory of these algebras will be one-based. In fact, any finitely based equational theory of algebras, which contains a reduct of algebras definitionally equivalent to the theory of all TBAs (or to the usual theory of all Boolean algebras) will always be one-based. Contrast this with the theory of Boolean groups (i.e., groups of exponent 2) with additional operators: given a natural number n, there exists an equational theory $B(n)$ containing a reduct of Boolean groups which is n based but not $n - 1$ based (see Theorem 2 of [8] for an actual construction of such equational theories). The same situation is true for the theory of all groups as well; this was announced without proof in [9].

References

[1] G. Gratzer. *Universal Algebra.* Springer Verlag, 2nd edition, 1979.

[2] A. A. Grau. Ternary boolean algebra. *Bull Amer. Math. Soc*, 53:567–572, 1947.

[3] D. Knuth and P. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebras*, pages 263–297. Pergamon Press, Oxford, U.K., 1970.

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

[5] 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.

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

[7] R. Padmanabhan and R.W. Quackenbush. Equational theories of algebras with with distributive congruences. *Proc. Amer. Math. Soc.*, 41:373–377, 1973.

[8] R. Padmanabhan and B. Wolk. Equational theories with a minority polynomial. *Proc. Amer. Math. Soc.*, 83:238–242, 1981.

[9] A. Tarski. Equational logic and equational theories of algebras. In K. Schütte, editor, *Contributions to Mathematical Logic*, pages 275–288. North-Holland, Amsterdam, 1968.