JOURNAL OF ALGEBRA 20, 78–82 (1972)

A Single Identity for Boolean Groups and Boolean Rings

N. S. MENDELSOHN AND R. PADMANABHAN

Department of Mathematics, University of Manitoba, Winnipeg, Canada

Received December 3, 1970

TO PROFESSOR RICHARD BRAUER, TO COMMEMORATE HIS SEVENTIETH BIRTHDAY, FEBRUARY 10, 1971

By a well-known result of Higman and Neumann, Boolean groups (i.e., groups of exponent 2) can be represented as the class of groupoids which satisfy a single identity. In this paper we find all minimal length single identities which characterize Boolean groups and represent Boolean rings (associative rings with unit satisfying $x^2 = x$) as the class of algebras with three operations and satisfying a single identity.

INTRODUCTION AND TERMINOLOGY

In this paper the terms groupoid and algebra will be given their present day interpretation in the sense of universal algebra; viz. a groupoid $\langle A; \circ\rangle$ is a system consisting of a set A together with a single binary operator $\circ$, while an algebra is a system $\langle A; f_1, f_2, ..., f_r\rangle$, where A is a set and $f_1, f_2, ..., f_r$ is a finite set of operators each being finitary. A class (short for equational class) of algebras is taken to mean the collection of algebras with a given set of operators and satisfying a finite set of identities. In Ref. [1], Higman and Neumann have shown that the class of groups is simply the class of all groupoids satisfying the identity

$$x \circ (((x^2 \circ y) \circ z) \circ ((x^2 \circ x) \circ z)) = y.$$

Here $x^2 = x \circ x$ and in terms of the ordinary group operation $x \circ y = xy^{-1}$. The above identity contains 10 symbols representing variables and we will say it is an identity of length 10. This is the shortest length of any identity which characterizes the class of all groups. In the same paper Higman and Neumann obtain the identity of length 6,

$$x \circ ((y \circ z) \circ (y \circ x)) = z,$$

which is a minimal length identity characterizing the class of Abelian groups. (A similar identity was obtained earlier by Tarski [3].) In Ref. [2], one of the present authors (Padmanabhan) obtains all minimal length identities characterizing Abelian groups.

Minimal Identities for Boolean Groups

Let $\mathscr{B}$ be the class of all Bolean groups. We characterize these groups by a single identity in terms of the group operation $\circ$. First, an identity $W_1 = W_2$ where W_1 and W_2 are words will not represent Boolean groups exclusively unless one of W_1 or W_2 is a single variable. Indeed, if $W_1 = W_1' \circ W_1''$ and $W_2 = W_2' \circ W_2''$, then $W_1 = W_2$ will be satisfied by a set F containing an element 0 such that $x \circ y = 0$ for every element in F. If the identity is $W = y$ where y is a variable and W is a word then W must contain the variable y since, otherwise, it is trivial that the only groupoid satisfied by such an identity must be on a set with only one element. Again, if in $W = y$ either the first or last variable in W is y, the identity is satisfied on any set where $x \circ y = y$ if y is the last letter of W or $y \circ x = y$ if y is the first letter of W. Hence, a necessary condition for $W = y$ to be an identity which represents Boolean groups is that W is a word in at least two variables and neither the first nor last letter of W is y. If W contains only two variables x and y, then it can easily be shown that $W(x, y) = y$ with the first and last letters of W being x cannot characterize Boolean groups. The proof, which is omitted here, consists of showing that for any such word W, a model of the identity can be found of the form $x \circ y = bx + (1 - b)y$, where x and y range over $GF(p)$ for some fixed prime p, and b is a fixed element in $GF(p)$ such that $b \neq 0, 1, \frac{1}{2}$. Such a groupoid is a quasigroup which is never commutative. We are now left with the situation where W contains three or more variables. The equation $W = y$ can be satisfied by Boolean groups only if each variable in W except y appears an even number of times and if y appears an odd number of times. Also if $W = y$ is to be satisfied only by Boolean groups and W contains three variables x, y, and z, the minimum length of W is 5 and a simple enumeration which takes into account that W does not start or end with y, shows that the maximum number of candidates for an appropriate identity $W = y$ is 126. This can be reduced to 63 by noting that if the identity $W = y$ is appropriate then so is $W^* = y$, where W^* is obtained from W by "reversing multiplication", i.e., defining $x * y = y \circ x$ and W^* is obtained from W by using the operator $*$ in place of $\circ$.

Minimal Identities for Boolean Groups

Theorem 1. *A groupoid $\mathfrak{A} = \langle A; + \rangle$ is a Boolean group, if and only if it satisfies the identity*

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

Proof. The "only if" part is obvious. Suppose now we have a groupoid satisfying (1). A sum $x + y$ can be replaced by an individual variable u by putting $y = ((x + t) + u) + t$. If we make this substitution in (1) we obtain the equation

$$x + ((u + z) + (((x + t) + u) + t)) = z. \tag{2}$$

In (2) put $z = ((u + v) + x) + v$ obtaining (after using (1)) the identity

$$x + u = ((u + v) + x) + v. \tag{3}$$

Pre-adding u to both sides of (3) and applying (1), we obtain

$$u + (x + u) = x. \tag{4}$$

In (1) put $y = x$ and using (4), we obtain

$$(x + x) + z = z. \tag{5}$$

Now pre-add z to both sides of (5) and using (4), we obtain

$$x + x = z + z \ (= 0 \text{ say}). \tag{6}$$

Thus special cases of (4) and (5), respectively, are

$$u + 0 = u \qquad \text{and} \qquad 0 + z = z. \tag{7}$$

Putting $v = 0$ in (3) and using (7), we obtain

$$x + u = u + x. \tag{8}$$

Finally, adding v to both sides of (3) and using (4) and (8) we get $(x + u) + v = x + (u + v)$; and this completes the proof of the theorem.

We state without proof the following result. All cases have a proof similar to that just given.

THEOREM 2. *The only groupoid identities of length* 6 *which characterize Boolean groups are the following* (*using concatenation for the groupoid operators*):

$$\begin{array}{rl}
(xy)((yz)x) = z, & (x(zy))(yx) = z, \\
x((zy)(xy)) = z, & ((xy)(xz))y = z, \\
x((zy)(yx)) = z, & ((xy)(yz))x = z, \\
(xy)(x(zy)) = z, & ((xz)y)(xy) = z, \\
(xy)(y(zx)) = z, & ((xz)y)(yx) = z, \\
x(y(x(zy))) = z, & (((xz)y)x)y = z, \\
x((x(yz))y) = z, & (x((zx)y))y = z, \\
x(((zy)x)y) = z, & (x(y(xz)))y = z, \\
x(((yz)x)y) = z, & (x(y(zx)))y = z, \\
x(((yx)z)y) = z, & (x(z(yx)))y = z, \\
x(((xy)z)y) = z, & (x(z(xy)))y = z.
\end{array}$$

We point out in passing that all 162 candidates have been examined, classified and interpreted. These results will appear in another paper by the authors.

A SINGLE IDENTITY FOR BOOLEAN RINGS

THEOREM 3. *Let $\mathfrak{A} = \langle A; f_1, f_2, \ldots, f_r\rangle$ be an algebra with one of the f_i being a binary operator, say $+$. Let $w(x_1, x_2, \ldots, x_n)$ be an arbitrary word in $\mathfrak{A}$, all the variables x_i being different from x, y or z. Then "$+$" is a Boolean group operation on A with $\mathfrak{A}$ satisfying the identity $w(x_1, x_2, \ldots, x_n) = 0$ (0 is the unit element of A under the operation $+$) if and only if $\mathfrak{A}$ satisfies the identity*

$$x + ((((x + y) + w) + z) + y) = z. \tag{9}$$

Proof. In (8), put $y = (((x + t) + w) + u) + t$ and noting that (8) itself implies $x + y = u$, Eq. (9) becomes

$$x + (((u + w) + z) + ((((x + t) + w) + u) + t)) = z. \tag{10}$$

Now put $z = (((u + w) + v) + w + x) + v$.

First notice that with this substitution (9) implies $(u + w) + z = x$ and using this fact in substituting for z in (10), we obtain

$$x + (x + ((((x + t) + w) + u) + t)) = ((((u + w) + v) + w) + x) + v.$$

Applying (8) again to this identity, we obtain

$$x = u = ((((u + w) + v) + w) + x) + v. \tag{11}$$

Again, in (10) put $x = (u + w) + z$ and using (8), we obtain

$$((u + w) + z) + u = z. \tag{12}$$

In (11), put $u = w$ and using (12) we have

$$x + w = (v + x) + v. \tag{13}$$

Put $x = w$ in (9) and using (13) we have

$$w + (((y + w) + z) + y) = z,$$

which, on using (12) reduces to

$$w + z = z. \tag{14}$$

Now put $u = w$ in (11) and using (14) and (12), we obtain

$$x + w = x.$$

From $x + w = x$, (9) becomes (1) and hence by Theorem 1, the operator $+$ defines a Boolean group operation in A. Hence, since by (14) with $z = w$, $w = w + w = 0$. Hence, the identity $w(x_1, x_2, \ldots, x_n) = 0$ holds in $\mathfrak{A}$.

THEOREM 4. *Boolean rings can be defined by a single identity.*

Proof. In Theorem 3, take $\mathfrak{A} = \langle A; +, \cdot, 1\rangle$, where $+$ and $\cdot$ are binary operators and 1 is a nullary operator and put

$$w(x_1, x_2, \ldots, x_8) = x_1^2 + x_1 + x_2(x_3 + x_4) + x_2x_3 + x_2x_4 + x_5 \cdot 1 + x_5 + (x_6x_7)\,x_8 + (x_7x_8)\,x_6 .$$

In the identity $w = 0$, we put each $x_i = 0$ except x_5 and using $u \cdot 0 = 0 + u = 0$, $u + u = 0$, we obtain

$$x_5 \cdot 1 + x_5 = 0$$

or, equivalently,

$$x_5 \cdot 1 = x_5 .$$

Now put $x_1 = 1$, $x_6 = x_7 = x_8 = 0$ in $w = 0$ to get

$$x_2(x_3 + x_4) = x_2x_3 + x_2x_4 .$$

Thus, $w = 0$ reduces to $x_1^2 + x_1 + (x_6x_7)\,x_8 + (x_7x_8)\,x_6 = 0$.
Again putting $x_6 = x_7 = x_8$ in the above identity we get the idempotent law $x_1^2 = x_1$ which yields $(x_6x_7)\,x_8 = (x_7x_8)\,x_6$. Finally, putting $x_8 = 1$ in the above we get the commutativity of the multiplication which in turn gives the associativity. This completes the proof of the theorem.

REFERENCES

1. G. HIGMAN AND B. H. NEUMANN, Groups as groupoids with one law, *Publ. Math., Debrecen* **2** (1952), 215–221.
2. R. PADMANABHAN, On single equational-axiom systems for Abelian groups, *J. Austral. Math. Soc.* **9** (1969), 143–152.
3. A. TARSKI, Ein Betrag zur Axiomatik der Abelian Gruppen, *Fund. Math.* **30** (1938), 243–256.