POSTULATES FOR BOOLEAN ALGEBRAS

MARLOW SHOLANDER

Introduction. The independence of postulates for well-known systems is a question of general interest. A closely related question is whether or not, by altering one or more of the postulates in an independent set, the set remains independent. From this standpoint the best sets of postulates are those which involve, first, the fewest postulates and, next, the least number of variables. As a rule progress is made in this direction at the sacrifice of simplicity of postulates. In this paper, in counting postulates, we ignore properties such as closure under the operations and count only identities or those stating that one equation implies another.

For Boolean algebras, sets of three postulates in three variables are common. We mention here only three particularly simple sets. The author's set [**11**] is of interest because two of the three postulates describe distributive lattices. Byrne [**5**] has an elegant set which consists of only two postulates if the postulate in the form of a double implication is not counted twice. A very simple set may be derived from Set IV of Huntington [**10**] by replacing commutativity and associativity by cyclic associativity (compare [**5**]).

Sets of two postulates are less common. Croisot [**7**] has one in five variables based on the ternary median operation and complements. Bernstein [**2**] has one in four variables based on the operation of implication. Bernstein [**1**] has a set in only three variables based on the stroke operation of Sheffer. Sets of two postulates based on ring operations have been given by Bernstein [**3**] and Byrne [**6**] but these involve seven and nine variables. In §§1 and 2 below we show that the number of variables may be reduced to four. This is made possible by the introduction of a single postulate for Boolean groups.

The only single postulate system for Boolean algebras that has been given is that of Hoberman and McKinsey [**9**]. It is hard to classify since it involves a single variable and a variable function. It may be regarded as an infinite set of postulates, all having the same form. In §3 below a single postulate system is given which involves five variables.

As an indication that near maximum condensation is being reached in these sets, we have the result of Diamond and McKinsey [**8**] showing that the use of at least three variables is necessary in describing Boolean algebras.

1. Boolean groups. In this and the next section we consider a set $\mathfrak{S}$ closed under addition. The following notation proves convenient. Let $a + b = (a, b)$, $a + (b, c) = (a, b, c)$ and, in general, $a + (b_1, b_2, \ldots, b_n) = (a, b_1, b_2, \ldots, b_n)$.

Received April 14, 1952. This paper was written while the author was under contract to the Office of Naval Research.

We assume the following identity holds in $\mathfrak{S}$:

P $$(a, b, c, b, c, b, a) = b.$$

It follows at once that

1.1 $$(a, b, a, b, a, b, a) = b.$$

1.2 $$(a + b) + a = b.$$

Proof. By P, notation, and 1.1,

$$\begin{aligned} b &= (a + b, b, a, b, a, b, a + b) \\ &= (a + b) + (b, a, b, a, b, a, b) \\ &= (a + b) + a. \end{aligned}$$

1.3 $$a + (b + a) = b.$$

Proof. By applying 1.2 twice

$$a + (b + a) = [(b + a) + b] + (b + a) = b.$$

1.4 $$c + (b + a) = (a + c) + b.$$

Proof. Starting with P and using 1.2,

$$\begin{aligned} (b, c, b, c, b, a) &= b + a, \\ (c, b, c, b, a) &= (b + a) + b = a, \\ (b, c, b, a) &= a + c, \end{aligned}$$

and $$(c, b, a) = (a + c) + b.$$

From 1.4, 1.2, and 1.3, we have

1.5 $$b = b + (a + a) = (a + a) + b.$$

1.6 $$a + a = b + b.$$

Proof. By 1.2 and 1.5, both sums equal $[b + (a + a)] + b$.

Denoting $a + a$ by O, we have $a + O = O + a = a$. Setting $c = O$ in 1.4, we obtain

1.7 $$a + b = b + a.$$

This, with 1.4, implies

1.8 $$a + (b + c) = (a + b) + c.$$

The proof that $\mathfrak{S}$ is a Boolean group is now complete.

2. Boolean rings. We now assume $\mathfrak{S}$ is closed under multiplication and satisfies, in addition to P, the identity Q given below. The symbol I found in postulate Q represents a fixed element of $\mathfrak{S}$.

https://doi.org/10.4153/CJM-1953-052-3 Published online by Cambridge University Press

Q $$(a,\ (cc)a,\ a(b+c),\ b(cd)) = (ba,\ (II)a,\ d(b+b),\ c(bd)).$$

We use freely the results of the previous section. In particular we note that equal terms may be cancelled if they occur on the same side or opposite sides of an equation.

If $a = d$ and $b = c$ we have from Q that

2.1 $$a + (bb)a = ba + (II)a.$$

Setting $b = I$ in 2.1 we obtain

2.2 $$a = Ia.$$

Hence $(II)a = Ia = a$ and from 2.1 we have

2.3 $$(bb)a = ba.$$

The previous results may be used to give Q the form

2.4 $$(ca,\ a(b+c),\ b(cd)) = (ba,\ dO,\ c(bd)).$$

Setting $a = b = I$ in 2.4 we have

2.5 $$cI + c = dO.$$

Setting $d = I$, we obtain

2.6 $$c = cI.$$

Equations 2.5 and 2.6 imply that

2.7 $$dO = O.$$

Equations 2.3 and 2.6 imply that

2.8 $$bb = b$$

Equation 2.7 may be used to give 2.4 the form

2.9 $$ca + a(b+c) + b(cd) = ba + c(bd).$$

Setting $d = O$, we have

2.10 $$a(b+c) = ba + ca.$$

This and 2.9 imply

2.11 $$b(cd) = c(bd).$$

Setting $d = I$ in 2.11 we find

2.12 $$bc = cb.$$

The last two identities show that multiplication is associative and commutative. Idempotence, the distributive law, and the role of I as a unit are given in 2.8, 2.10, and 2.2. Thus [**4**, p. 154], $\mathfrak{S}$ is a Boolean ring with unit or a Boolean algebra.

3. A single postulate. We consider a set $\mathfrak{S}$ closed under an operation denoted by a vertical bar. It is convenient to introduce primes to denote

https://doi.org/10.4153/CJM-1953-052-3 Published online by Cambridge University Press

"squares." Thus $a' = a|a$, $a'' = (a')'$ and so on. It is assumed $\mathfrak{S}$ satisfies the following postulate:

R $\qquad (x|(y'|y))'' = (a|(b'|c))''$ implies that $x = (b|a)|(c'|a)$.

If we set $a = x$, $b = c = y$, we obtain

3.1 $$x = (y|x)|(y'|x).$$

Setting $y = x$ we have

3.2 $$x = x'|(x'|x).$$

3.3 $$(a|(b'|c))' = (b|a)|(c'|a)$$

Proof. Set $x = a \mid (b' \mid c)$. By 3.2, $(x' \mid (x' \mid x))'' = (a \mid (b' \mid c))''$. By R, $x' = (b|a)|(c'|a)$.

From 3.1 and 3.3 we have

3.4 $$x = (x|(y'|y))'.$$

3.5 $$x' = y' \text{ implies } x = y.$$

Proof. If $x' = y'$ we have from 3.4 that $(x|(x'|x))'' = (y|(y'|y))''$. By R and 3.2, $x = (y|y)|(y'|y) = y$.

3.6 $$x|(y'|y) = x|(z'|z)$$

Proof. By 3.4, since both terms equal x, $(x|(y'|y))' = (x|(z'|z))'$. We now apply 3.5.

3.7 $$(x|x'')' = x'|(x''|x).$$

Proof. Since $x'' = x'|x'$ this is a consequence of 3.3.

3.8 $$x|x'' = x'.$$

Proof. By 3.7 and 3.3, $(x|x'')'' = (x'|(x''|x))' = (x'|x')|(x'|x') = x'''$. We now apply 3.5.

3.9 $$x''|x = x'$$

Proof. By 3.3 and 3.7, $(x''|x)'' = ((x''|x)|(x''|x))' = (x'|(x''|x))' = (x|x'')''$. We now apply 3.5 and 3.8.

3.10 $$x|x' = x'|x.$$

Proof. By 3.9 and 3.3, $(x|x')' = (x|(x''|x))' = (x'|x)'$. We now apply 3.5.

3.11 $$x'' = x.$$

Proof. By 3.4, 3.3, 3.8, 3.10, 3.6, and 3.2, $x'' = (x''|(x'|x))' = (x|x'')|(x'|x'') = x'|(x'|x'') = x'|(x''|x') = x'|(x'|x) = x$.

https://doi.org/10.4153/CJM-1953-052-3 Published online by Cambridge University Press

3.12 $$x|y = y|x.$$

Proof. $x|y = (x|(y'|y'))'' = ((y|x)|(y''|x))' = (y|x)'' = y|x.$

Identities 3.11, 3.4, and 3.3 are clearly equivalent to Sheffer's three postulates and these together with 3.12 to Bernstein's two postulates [**1**]. Thus $\mathfrak{S}$ is a Boolean algebra under the operations defined by $x + y = (x|y)'$ and $xy = x'|y'$. It is not unlikely that a variation of R would give a single Boolean algebra postulate expressed in terms of complements and either meets or joins.

References

1. B. A. Bernstein, *Simplification of the set of four postulates for Boolean algebras in terms of rejection*, Bull. Amer. Math. Soc., *39* (1933), 783–787.

2. ———, *A set of four postulates for Boolean algebra in terms of the "implicative" operation*, Trans. Amer. Math. Soc., *36* (1934), 876–884.

3. ———, *Postulate-sets for Boolean rings*, Trans. Amer. Math. Soc., *55* (1944), 393–400.

4. Garrett Birkhoff, *Lattice theory*, 2nd ed. (New York, 1948).

5. Lee Byrne, *Two brief formulations of Boolean algebra*, Bull. Amer. Math. Soc., *52* (1946), 269–272.

6. ———, *Short formulations of Boolean algebra using ring operations*, Can. J. Math., *3* (1951), 31–33.

7. R. Croisot, *Axiomatique des lattices distributives*, Can. J. Math., *3* (1951), 24–27.

8. A. H. Diamond and J. C. C. McKinsey, *Algebras and their subalgebras*, Bull. Amer. Math. Soc., *53* (1947), 959–962.

9. S. Hoberman and J. C. C. McKinsey, *A set of postulates for Boolean algebra*, Bull. Amer. Math. Soc., *43* (1937), 588–592.

10. E. V. Huntington, *New sets of independent postulates for the algebra of logic*, Trans. Amer. Math. Soc., *35* (1933), 274–304 with corrections 557 and 971.

11. Marlow Sholander, *Postulates for distributive lattices*, Can. J. Math., *3* (1951), 28–30.

Washington University

https://doi.org/10.4153/CJM-1953-052-3 Published online by Cambridge University Press