DISTRIBUTIVE POSTULATES FOR SYSTEMS LIKE BOOLEAN ALGEBRAS

BY

GEORGE D. BIRKHOFF AND GARRETT BIRKHOFF

1. **Introduction.** Boole [2, p. 41][1] pointed out a close analogy between ordinary algebra and the "algebra of logic," now called Boolean algebra. Both have operations of addition and multiplication which are commutative and associative; both have a 0 for addition and multiplication and a 1 for multiplication; in both, multiplication is distributive on sums.

The connection was first made precise by Stone [5]. Stone defined a "Boolean ring" as a ring in which $aa=a$, and showed that this implies $a+a=0$ and $ab=ba$. He showed that by simple constructions, one could transform Boolean algebras into Boolean rings and vice versa.

Stone and most earlier authors (see Huntington [3]) used commutative and associative laws. In a remarkable paper [4], Newman based his developments entirely on distributivity, the existence of complements, and the properties of 0 and 1. Every such distributive, complemented algebra is the direct sum of the *Boolean subalgebra* of elements satisfying $a+a=a$, and the (not necessarily associative) *Boolean subring* of elements satisfying[2] $a+a=0$.

During lectures on Boolean algebra, but using stronger postulates, G. D. Birkhoff independently discovered Newman's decomposition theorem. Our discussion of this in the summer of 1944 led to the results presented below.

As Newman's postulates are independent (cf. J. London Math. Soc. vol. 17 (1942) pp. 34–47 and vol. 14 (1944) pp. 28–30), we have been unable to weaken them. However, we have been able to make large parts of his argument much shorter and simpler, at the cost of a weak additional postulate (P3$'$ below), added to those of his Theorem 1b. We show that one need only apply Boole's method of expansion [2, p. 151], systematically.

We first show (§2) that the postulates are left-right symmetric by a new and simple argument. We then show (§3) that the existence and properties of "even" elements follow from more general considerations than those of Newman, and give (§4) a simplified proof of his decomposition theorem. In §5, we give a new set of postulates for distributive lattices; in §6, we give an

Presented to the Society, February 23, 1946; received by the editors December 5, 1945.

[1] Numbers in brackets refer to the Bibliography at the end of the paper.

[2] It is easily shown that any "idempotent" ring (in which $aa=a$ for all a) satisfies $a+a=0$ and $ab=ba$; the proof of [5] applies to the nonassociative case. Conversely, in any such ring, $a+1$ is a complement of a. Finally, any idempotent and commutative multiplication table for basis-elements defines an idempotent ring (cf. L. E. Dickson, *Algebras and their arithmetics*, Chicago, 1922, p. 22); the idempotence follows from the binomial theorem and commutativity.

entirely novel approach to postulates for Boolean algebras and (associative) Boolean rings. Finally, in §7, we show that in addition to the "metamathematical" principles of duality and left-right symmetry, only three postulates are needed for Boolean algebras and three for distributive lattices—but that two are not quite enough.

2. Postulates; first deductions. Consider any system with two binary operations which satisfies the following postulates:

P1. $a(b+c)=ab+ac$. P1'. $(a+b)c=ac+bc$.

P2. $\exists 1$, such that $a1=a$ for all a.

P3. $\exists 0$, with $a+0=a$. P3'. $0+a=a$.

P4. To each a corresponds at least one a', such that $aa'=0$ and $a+a'=1$.

That is, multiplication is *distributive* on sums, we have a *multiplicative right-unit*, an *additive zero*, and *right-complements*. We shall now show that multiplication is idempotent, that complementation is involutory and unique, that right-complements are left-complements, that the multiplicative right-unit is also a left-unit, and that the additive zero is also a multiplicative zero. The postulates which are superfluous in each proof are listed to the right of the statement of the result.

T1. $aa=a$. (Cf. [4, p. 1].) (*without* P1', P3').

Proof. $a=a1=a(a+a')=aa+aa'=aa+0=aa$.

T2. $(a')'=a$ *for all* a *and* $(a')'$. (Cf. [4, p. 3].)

Proof.

$$\begin{aligned}(a')' &= 0 + (a')'(a')' && \text{by P3}', \text{T1}\\ &= a'(a')' + (a')'(a')' = (a' + (a')')(a')' \\ &= 1(a')' = (a + a')(a')' = a(a')' + 0 && \text{by P4}\\ &= 0 + a(a')' = aa' + a(a')' = a(a' + (a')') \\ &= a\cdot 1 = a.\end{aligned}$$

Remark. Without using P2, we have shown that $(a')'=a\cdot(a')'=a\cdot 1$.

COROLLARY 1. $a'a=0$ *and* $a'a=1$.

COROLLARY 2. *If* $ab=ac=0$ *and* $a+b=a+c=1$, *then* $b=c$; *complements are unique.*

For if a' is any complement of a, $b=((a')')'=c$.

COROLLARY 3. $1\cdot a=a$, for all a.

Proof. $1\cdot a=(a+a')a=aa+a'a=a+0=a$.

T3. $a\cdot 0=0\cdot a=0$, *for all* a.

Proof. $0=aa'=a(a'+0)=aa'+a0=0+a0=a0$, and $0=aa'=(0+a)a'$

$=0a'+aa'=0a'+0=0a'$, all without using P2. But by T2 every element is a complement; hence $0a'=0$ for all a implies $0a=0$ for all a.

COROLLARY. *If* $0=1$, *then* $0=0+0=0+a\cdot 0=0+a\cdot 1=a\cdot 1=a$; *hence all elements are equal.*

Remark. By T2, Corollary 1, which is symmetric to P4, and T2, Corollary 3, which is symmetric to P2, we now have *complete left-right symmetry* in the properties of addition and multiplication.

An easier way to guarantee this would of course be to substitute the commutative laws $ab=ba$ and $a+b=b+a$ for P1′ and P3′.

3. **Even elements.** We now define $1+1=2$, $2+2=4$, and call the left-multiples $y2$ of 2 *even* elements. This is the opposite of Newman's usage. We note that by P1, P2 and T1 alone, $4=2+2=2\cdot 1+2\cdot 1=2(1+1)=2\cdot 2=2$; also, by definition, $4=(1+1)+(1+1)$.

T4. *An element x is even if and only if it is additively idempotent*: $x+x=x$ (*without* P1′, P3′).

Proof. Clearly $y2+y2=y(2+2)=y2$; conversely, if $x=x+x$, then $x=x\cdot 1+x\cdot 1=x(1+1)=x2$.

T5. *Any multiple xt or ux of an even element x is even.*

Proof. If $x=x+x$, then $xt=(x+x)t=xt+xt$ and $ux=u(x+x)=ux+ux$ for all t, u.

T6. *The correspondence $x\rightarrow x+x=x2$ is an idempotent endomorphism*; *that is*, $(x+y)2=x2+y2$, $(xy)2=(x2)(y2)$, *and* $(x2)2=x2$ (*without* P3′).

Proof. By P1′, $(x+y)2=x2+y2$. Again, $(x2)2=x2+x2=x(2+2)=x2$ by P1, P2, T1. Finally, by P1, P1′, P2, T1

$$\begin{aligned}(x2)(y2) &= (x+x)(y+y) = (x+x)y+(x+x)y = (xy+xy)+(xy+xy)\\ &= ((xy)2)2 = (xy)2.\end{aligned}$$

It is a corollary of T6 that the *even elements form a subalgebra*, in which addition is idempotent.

We remark that T4–T6 not only do not require P3′, but only require P3–P4 insofar as they are needed to prove T1. That is, T4–T6 are valid in any system with idempotent multiplication and a right-unit, in which the distributive laws P1–P1′ are valid. These considerations are developed further in §7.

4. **Direct decomposition theorem.** Now let $2'$ denote the right-complement of 2, so that $2\cdot 2'=0$, $2+2'=1$; we shall call the left-multiples of $2'$, *odd* elements. Using the results of §2, it is easy to obtain a direct decomposition theorem.

T7. *The odd elements are the additively nilpotent elements. More precisely, the conditions* $x=y2'$, $x=x2'$, $x+x=x2=0$ *are equivalent.*

Proof. If $x+x=0$, then $x=x(2+2')=x2+x2'=0+x2'=x2'$. If $x=x2'$, then $x=y2'$ trivially, all without P3. Finally, $y2'+y2'=y(2'+2')=y(2'\cdot 2)$ $=y0=0$ by T2, Corollary 1, and T3. We remark that T7 follows if we have a right unit 1, a right-additive and right multiplicative zero, right distributivity, and left-complements.

T7′. *Any multiple of an odd element is odd.*

Proof. If $x+x=0$, then $xt+xt=(x+x)t=0t=0$, and $ux+ux=u(x+x)$ $=u\cdot 0=0$ for all t, u, by P1, P1′, T3.

T8. *Any system satisfying* P1, P1′, P2, P3, P3′, P4 *is the direct union of the subalgebras of even and odd elements.*

Proof. Consider the correspondences $z\rightarrow(z2, z2')=(x, y)$ and $(x, y)\rightarrow x+y$. If x is even and y is odd, then

$$(x+y)2 = x2+y2 = (x+x)+0 = x \qquad \text{by P1, T7, P3,}$$

$$(x+y)2' = x2'+y2' = (x+x)2'+y = y \qquad \text{by P1, P3}',$$

since $(x+x)2'=x2'+x2'=x(2'+2')=x0=0$. Conversely, for any z, $z2$ is even and $z2'$ odd, and $z=z\cdot 1=z(2+2')=z\cdot 2+z2'$. Hence the correspondences are one-one and reciprocal. Further, $(z+z_1)2=z2+z_12$ and $(z+z_1)2'=z2'+z_12'$; hence addition is component-by-component. Finally,

$$\begin{aligned}(x+y)(x_1+y_1) &= (xx_1+xy_1)+(yx_1+yy_1) && \text{by P1–P1}'\\ &= (xx_1+0)+(0+yy_1) && \text{as shown below}\\ &= xx_1+yy_1 && \text{by P3–P3}'.\end{aligned}$$

(To show that $xy_1=yx_1=0$, note that xy_1 and yx_1 are both even and odd by T5, T7′; while if u is both even and odd, then $u=u+u=0$ by definition and T7.) Hence multiplication is also component-by-component, xx_1 being even and yy_1 odd by T5, T7′.

We can now prove that *the even elements form a Boolean algebra,* while *the odd elements form a* (*not necessarily associative*) *ring, in which multiplication is commutative and idempotent.* But as we have nothing to add to Newman's proof, we shall not repeat his argument[3].

5. **Postulates for distributive lattices.** Instead, we shall give a new proof that the even elements form a Boolean algebra, which will yield as a by-product a new set of postulates for distributive lattices. By confining ourselves to even elements, we have the additional postulate

[3] One can show successively $a+1=1+a$, $a+b=b+a$, $1+(1+c)=(1+1)+c$, $1+(b+c)$ $=(1+b)+c$, $a+(b+c)=(a+b)+c$; the trick is to right-multiply respectively by $a+a'$, $b+b'$, $c+c'$, $b+b'$, $a+a'$ and expand. Cf. [4, p. 260].

P5. $a+a=a$.
Using this, we can show

T9. $a+1=1+a=1$.

Proof. By P2–T2, P1–P1′, T1, T4=P5, and P3′, we have

$$a+1=(a+1)(a+a')=(aa+1a)+(aa'+1a')$$
$$=(a+a)+(0+a')=a+a'=1.$$

By symmetry (§2), we get $1+a=1$.

We shall now show that *any system which satisfies* P1–P1′, P2–P2′, T1, *and* T9 *is a distributive lattice with* 1. It is a corollary that the even elements in any system satisfying P1–P1′, P2, P3–P3′ and P4 form a Boolean algebra (complemented distributive lattice). We shall prove the usual postulates for a distributive lattice as a chain of identities.

T10. $a+a=a$.

Proof. By P2, T9, P1, T1, and with P5, we have $a=a1=a(a+1)=aa+a\cdot 1=a+a$.

T11. $ab+a=a+ab=a+ba=ba+a=a$.

Proof. $a+a\cdot 1=a(b+1)=ab+a1=ab+a$. The other proofs are entirely similar.

T12. $a(a+b)=a(b+a)=(a+b)a=(b+a)a=a$.

Proof. $a(a+b)=aa+ab=a+ab=a$, by P1, T1, T11. The other proofs are entirely similar.

T13. $a+b=b+a$.

Proof. By T12, P1, P1′, T12, we have

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

T14. $a[(a+b)+c]=a$, $b[(a+b)+c]=b$, $c[(a+b)+c]=c$.

Proof. By P1, T12, and T1, we have

$$a[(a+b)+c]=a(a+b)+ac=a+ac=a,$$
$$b[(a+b)+c]=b(a+b)+bc=b+bc=b,$$
$$c[(a+b)+c]=c(a+b)+cc=c(a+b)+c=c.$$

T15. $a+(b+c)=(a+b)+c$.

Proof. $a+(b+c)=a[(a+b)+c]+(b[(a+b)+c]+c[(a+b)+c])$ by T14.

By P1′, this is $[a+(b+c)][(a+b)+c]$. By left-right symmetry, this can be shown to be $(a+b)+c$.

T16. *$a+bc=(a+b)(a+c)$ and $ab+c=(a+c)(b+c)$.*

Proof. By P1–P1′, T1, T12, T15, and T11, we have

$$(a+b)(a+c) = a(a+c) + b(a+c) = a + (ba + bc)$$
$$= (a + ba) + bc = a + bc.$$

The other identity follows by symmetry.

We now define the *dual* of an identity to be the equality obtained from it by interchanging addition and multiplication. Thus P1–P1′ and T16 are dual; T1 and T10 are dual; T11 and T12 are dual. Since the proofs of T13 and T15 involve only these laws, it follows that *dual proofs can be made to show*

T17. *$ab=ba$.*

T18. *$a(bc)=(ab)c$.*

But T1, T10, T17, T13, T18, T15, T12, T13, and P1–P1′ are the usual postulates for a distributive lattice; this completes our demonstration.

Remark. 1. Since the postulates for a distributive lattice are self-dual, it follows that T16, P3–P3′, $a0=0a=0$, and T10 are postulates for a distributive lattice with zero.

Remark 2. Just after T12, we can easily show that the conditions $a+b=a$, $b+a=a$, $ab=b$, and $ba=b$ are all equivalent to each other—and hence define $a \geqq b$ in a self-dual manner. We can show $a \geqq a$, that $a \geqq b$ and $b \geqq a$ imply $a=b$. But we need T15 or T18 to prove transitivity.

6. **Subdirect decomposition theorem.** We shall now use an entirely different and shorter argument to characterize the most general direct union of a Boolean algebra and an associative Boolean ring.

THEOREM. *The most general algebra satisfying* P1–P1′, P2–P2′, P3, P4, *and* P6, $(ab)c=(ac)(bc)$, *is a direct union of a Boolean algebra and an associative Boolean ring.*

Proof. Each identity is valid in every homomorphic image of an algebra A, if it is valid in A. It is also valid in the direct union $A \oplus B$, if it is valid in A and B individually. Hence it is valid in any *subdirect union* (in the sense of [1]) of algebras in which it holds. It follows, by the principal conclusion of [1], that all consequences of these identities which hold in every *subdirectly irreducible* algebra satisfying them, hold in *every* algebra satisfying them.

But now observe that (by definition) every correspondence $x \rightarrow xa$ of an algebra A is an *endomorphism,* if and only if P1′, P6 hold.

LEMMA 1. *Any algebra which satisfies* P1–P1′, P2–P2′, P3, P4, P6, *and contains an element a not* 0 *or* 1, *is subdirectly reducible.*

Proof. Since the correspondences $x \to xa$, $x \to xa'$ are endomorphisms (P1′, P6), the correspondence $x \to (xa, xa')$ is a homomorphism of A onto a subdirect union. Since $xa = ya$ and $xa' = ya'$ imply (P2, P4, P1)

$$x = x1 = x(a + a') = xa + xa' = ya + ya' = y(a + a') = y1 = y,$$

this homomorphism is an isomorphism. Again, by T1, $aa = a$ and by P2′, $1a = a$ $(a \neq 1)$, while $a'a' = a'$ and $1a' = a'$ similarly, where $a' = 1$ would imply $0 = aa' = a1 = a$, contrary to hypothesis. Hence both endomorphisms determine proper congruence relations, and A is subdirectly reducible.

LEMMA 2. *The only algebras consisting of* 0 *and* 1 *which satisfy* P1–P1′, P2–P2′, P3, P4, P6 *are the Boolean algebra of two elements and the Boolean ring of two elements.*

Proof. By P2, P2′, P3, we have

$$0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1, \quad 0 + 0 = 0, \quad 1 + 0 = 1. \tag{1}$$

Since $0 + 0 = 0$, $0'$ cannot be 0 and must be 1. This gives, by P4,

$$0 + 1 = 1. \tag{2}$$

Again, $0 \cdot 0 = 1$ would imply the contradiction

$$1 = 0 \cdot 0 = (1 \cdot 0) \cdot 0 = (1 \cdot 0) \cdot (0 \cdot 0) \text{ (by P6) } = 0 \cdot 1 = 0;$$

hence $0 \cdot 0 = 0$. The only sum or product not determined is $1 + 1$; the possibilities $1 + 1 = 1$ and $1 + 1 = 0$ give the two cases mentioned in Lemma 2.

COROLLARY. *Any algebra satisfying* P1–P1′, P2–P2′, P3, P4, *and* P6 *is a subdirect union of Boolean algebras and Boolean rings of two elements.*

It is a further corollary that addition and multiplication are commutative and associative, and indeed that all the results of §§2–4 hold.

Remark 1. We can replace P2′ by $0a = 0$ in the preceding argument: in the proof of Lemma 1, $0a' = aa' = 0$, where $0 \neq a$, and $(a')(a')' = 0 = 0(a')'$, where $a' = 0$ would imply $a = a + a' = a + 0 = 1$, hence $x \to (xa', x(a')')$ subdirectly reduces A. In Lemma 2, $1 \cdot 0 = 0$ is lost in (1); but since $1 \cdot 1 = 1$, $1' \neq 1$, hence $1' = 0$ and $1 \cdot 0 = 1 \cdot 1' = 0$ still holds.

Remark 2. Thus replacing P3′ in §2 by P6 and P2′ or $0a = a$ effectively guarantees that the odd elements form an *associative* ring; otherwise it has no effect.

Remark 3. We can prove analogous results for systems satisfying P1, P2, P3′, T9, P6, $ab + c = (a + c)(b + c)$, $(a + c) + (b + c) = (a + b) + c$ and the commutative law of multiplication. By assumption, the correspondences $x \to xa$ and $x \to x + a$ are endomorphisms, for all a. Again, $a = (1 \cdot 1)a = (1a)(1a) = aa$. It follows that if $xa = ya$ and if $x + a = y + a$, then

$$x = x1 = x(1 + a) = x + xa = xx + xa = x(x + a) = x(y + a)$$
$$= xy + xa = yx + ya = y(x + a) = y(y + a) = y.$$

Thus the correspondence $x \rightarrow (xa, x+a)$ is a *isomorphism*. Again $1a = aa$ and $0+a = a = a(1+1) = a+a$; hence any system containing an $a \neq 0$, 1 is subdirectly reducible. And the only system of 0 and 1 satisfying our postulates is a distributive lattice.

7. **Self-dual and symmetric postulates; counterexamples.** We have already observed that the laws of Boolean algebra are left-right symmetric for addition and multiplication (§2, Remark), and self-dual under interchange of addition and multiplication (§5, Remark 1). Thus they are invariant under an *octic group* of symmetries[4]. The same remark applies to distributive lattices.

This suggests introducing the group of symmetries on the postulates as a "metamathematical" postulate, and seeing how few other postulates are required. It is evident that the following *three* are sufficient for Boolean algebra:

P1. $a(b+c) = ab+ac$. P2. $a1 = a$. P4. $a+a' = 1$.

For we get P1, P1′, P2, P3, P3′, P4 immediately, and from T1, by dualization, we get $a+a = a$.

This easy success suggests trying to see whether P1, P2, and their transforms under the octic group of left-right symmetries and duality do not constitute a sufficient set of postulates for a distributive lattice. In fact, one can prove directly that

$$1 = 0 + 1 = (0 \cdot 1) + 1 = (0 + 1)(1 + 1) = 1 \cdot (1 + 1)$$
$$= 1 \cdot 1 + 1 \cdot 1 = 1 + 1,$$

by the dual-symmetric P3′ of P2, P2, the dual-symmetric of P1, P3′ again, P1, and P2 respectively. Multiplying through by a (using P2), and dualizing, we get *idempotence*:

$$a + a = a, \qquad aa = a. \tag{1}$$

Furthermore, consider the "free algebra" generated by 0, 1, a. Let $s, s_1, s_2, \cdots$ denote generically *sums* of terms 1 and a, and $p, p_1, p_2, \cdots$ denote dually *products* of terms 0 and a. We can prove by induction that all elements other than 0, 1, a are such sums or products.

Indeed, from the cases $s = 1$ and $s = a$, it follows by induction since $a(s+s_1) = as+as_1$ and $a+a = a$ that

$$as = sa = a, \quad \text{whence} \quad a + p = p + a = a, \tag{2}$$

[4] This is in accordance with the philosophic principle that "The final form of any scientific theory T is (1) based on a few simple postulates, and (2) contains an extensive ambiguity, associated symmetry, and underlying group G, in such wise that . . . T appears nearly self-evident in view of the Principle of Sufficient Reason." (G. D. Birkhoff)

by duality. We shall now prove that

$$sp = ap = p_1 \qquad (s \neq 0, 1). \tag{3}$$

Indeed, $ap=ap$, $(s+1)p=sp+p=ap+pp$ (by induction and (1)) $=(a+p)p$ $=ap$ by (2), and $(s+s')p=sp+s'p=ap+ap$ (by induction) $=ap$ by (1). This completes the proof of (3). By duality, we get

$$s + p = s + a = s_1 \qquad (s \neq 0, 1). \tag{4}$$

Since $s+s=ss=s$ and $p+p=pp=p$, we have a homomorphism of the "free algebra" onto the system with five elements 0, 1, a, s, p and the rules of operation described by P1, P2, (1)–(4) and their left-right symmetric and dual transforms. This self-dual and symmetric image algebra however satisfies P1, P2; hence P1, P2 *and their transforms do not constitute a set of postulates for distributive lattices.* (Though by §5, P1, P2, and T9 and their transforms do.)

An even more simple counterexample consists of two elements: $0=1$ and a, with identical addition and multiplication tables given by:

$$00 = 0 + 0 = 0,$$
$$0a = a0 = 0 + a = a + 0 = aa = a + a = a.$$

In this system, addition and multiplication are idempotent, commutative, and associative; all distributive laws hold; 0 is an additive and 1 a multiplicative unit; a is a multiplicative zero and additive unity. Moreover by forming the direct product of it and the Boolean algebra of two elements, we can make $0\neq 1$.

It would be interesting to determine what were the different elements of the form s and p in the "free" self-dual and symmetric algebra generated by a (with 0 and 1) subject to P1 and P2.

It would also be interesting to determine the independent subsets of the postulates (for distributive lattices) generated by P1, P2, T9 and their transforms under the octic group of left-right symmetries and duality.

Bibliography

1. G. Birkhoff, *Subdirect unions in universal algebra*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 764–768.

2. George Boole, *The laws of thought*, 1854, republished by the Open Court Publishing Co.

3. E. V. Huntington, *New sets of independent postulates for the algebra of logic*, Trans. Amer. Math. Soc. vol. 35 (1933) pp. 274–304; corrections on pp. 557, 971.

4. M. H. A. Newman, *A characterization of Boolean algebras and rings*, J. London Math. Soc. vol. 16 (1941) pp. 256–272.

5. M. H. Stone, *Representations of Boolean algebras*, Trans. Amer. Math. Soc. vol. 40 (1936) pp. 37–111.

Harvard University,
Cambridge, Mass.