AUTOMETRIZATION AND THE SYMMETRIC DIFFERENCE

J. G. ELLIOTT

1. Introduction. The fact that the symmetric difference (i.e., $ab' + a'b$) is a group operation in a Boolean algebra is, of course, well known. Not so well known is the fact observed by Ellis [3] that it possesses some of the desirable properties of a metric distance function. Specifically, if $*$ denotes this operation, it is easy to verify that

M1: $a * b = 0$ if and only if $a = b$,

where 0 is the first element of the Boolean algebra,

M2: $a * b = b * a$,

M3: $(a * b) + (b * c) > (a * c)$,

where $>$ denotes inclusion in the wide sense. In this note $a + b$ and ab denote respectively the join and meet of a and b. Any binary operation satisfying M1, M2, and M3 might be referred to appropriately as an autometric operation, or simply as a metric operation. It might be observed that, in the language of Ellis [4], these properties make the Boolean algebra into a generalized metric ground space. The symmetric difference is at once a group and a metric operation. Our first objective in this note is to prove that the symmetric difference is the only such operation. We then examine other possible characterizations of the symmetric difference arising from weakening or changing these hypotheses.

By way of historical summary we observe that Bernstein [**1**; **2**] characterized the possible group operations in a Boolean algebra among the class of Boolean operations and Frink [**5**] characterized the symmetric difference, again among the class of Boolean operations, as the only group operation over which the set product distributes. More recently Helson [**7**] and Marczewski [**8**] have characterized the symmetric difference as the only group operation satisfying certain other side conditions.

2. Metric operations. In this section we designate by $*$ a binary operation which is simultaneously a group operation and a metric operation in a Boolean algebra, and proceed to identify the operation with that of the symmetric difference.

THEOREM 2.1. *The only metric group operation in a Boolean algebra is the symmetric difference.*

Received April 6, 1952. This paper is part of a doctoral study. The author is indebted to Professor L. M. Kelly for his helpful suggestions and guidance in the preparation of this paper.

Proof. If x, y, and z are the sides of a triangle in the Boolean algebra, then $x + y = x + z = y + z$. For $x + y > z$ and $x + z > y$ by M3, and upon adding x to each side of each expression, we find $x + y > x + z$ and $x + z > x + y$. This implies that $x + y = x + z$. The proof is similar for the other cases.

Suppose now that $a = b * c$. From M1 and the associativity of $*$, it follows that $0 = a * (b * c) = (a * b) * c$, and hence $a * b = c$. Thus if $a * b = c$, then $a * c = b$ and $b * c = a$. It follows immediately that $0 * a = a$, for if we assume that $0 * a = b$, then $a * b = 0$ by the previous statement. Thus $a = b$ by M1.

We now show that $a * I = a'$, where a' denotes the complement of a. Let $a * a' = b$, and consider the triangle $0, a, a'$. Now $a + b = a + a' = I$, and $a' + b = a + a' = I$, so $I = (a + b)(a' + b) = b$. Thus $a * a' = I$, and $a * I = a'$ follows immediately.

Let $x * y = p$. We will show that $p = xy' + x'y$. From the quadrilateral $0, I, x, y$ we see that $x' + y' = x' + p$ and $x' + y' = y' + p$. Hence $xy' = xp$ and $x'y = yp$. We then have $xy' + x'y = (x + y)p = p$, since $x + y > p$ by M3. This proves the theorem.

Noting that no use was made of the identity and inverse postulates of a group, we immediately have

THEOREM 2.2. *The only metric semi-group operation in a Boolean algebra is the symmetric difference.*

DEFINITION. An operation $*$ is said to be *weakly associative* if

$$a * (a * b) = (a * a) * b.$$

THEOREM 2.3. *The only metric weakly associative operation in a Boolean algebra is the symmetric difference.*

Proof. In Theorem 2.1, we note that the full power of the associative law was used only to show that if $a = b * c$ then $b = a * c$ and $c = a * b$. These results follow from the weak associative law and the metricity of the operation, for let $b * c = a$, $a * b = x$ and $a * c = y$. Then

$$x = b * a = b * (b * c) = (b * b) * c = 0 * c = c,$$

$$y = c * a = c * (c * b) = (c * c) * b = 0 * b = b.$$

Associativity was used strongly in the preceding theorems, but is not used in the following theorem.

DEFINITION. A *quasigroup* is a system consisting of a set of elements, together with a binary operation which satisfies the law of unique solution. That is, if $a = b * c$ and two of these symbols are known, then the third is uniquely determined. A loop is a quasigroup with a two-sided identity element.

DEFINITION. The *Ptolemaic inequality* holds for a quadrilateral if the three products (meets) of opposite sides satisfy the triangle inequality (M3).

https://doi.org/10.4153/CJM-1953-037-7 Published online by Cambridge University Press

THEOREM 2.4. *The only metric loop operation in a Boolean algebra is the symmetric difference.*

Proof. Let the loop identity be called e. Since $e * e = e$ by the identity law, and $e * e = 0$ by M1, it follows that $e = 0$. We now show that $a * I = a'$. By the law of unique solution there exists an element y such that $a * y = a'$. Consider the triangle 0, a, y. By the triangle inequality we have

$$a + y > a' \quad \text{and} \quad a' + y > a.$$

Thus

$$aa' + ya' > a'a' \quad \text{and} \quad a'a + ya > aa,$$

whence $y > a'$ and $y > a$. Hence $y = I$, as the only element which is over both a and a' is I.

We now show that the Ptolemaic inequality holds for any quadrilateral 0, I, a, b. Letting $a * b = x$, we have $0 * a = a$, $0 * I = I$, $I * a = a'$, and $I * b = b'$. The triangle inequality for triangle 0, a, b yields $a + b > x$. Again, the triangle inequality for triangle I, a, b yields $a' + b' > x$. Hence $(a + b)(a' + b') > xx$ or $ab' + a'b > x$. The other two cases are proved equally easily.

Now let $a * b = x$. We wish to show that $x = ab' + a'b$. We have just found that $ab' + a'b > x$. Consider the quadrilateral 0, I, a, b'. By the Ptolemaic inequality, we have $ab + a'b' > (a * b')$. Hence

$$(ab' + a'b)(ab + a'b') > x(a * b')$$

or $0 > x(a * b')$, so $x(a * b') = 0$. By the triangle inequality, $x + (a * b') > I$, thus

$$x + (a * b') = I.$$

Hence $x' = a * b'$ by the definition of complement. In the same manner we show that $x' = a' * b$ and $x = a' * b'$. From the triangle I, a', b we obtain $a' + b > x'$, and from the triangle I, a, b' we obtain $a' + b > x'$. Hence

$$(a + b')(a' + b) = ab + a'b' > x'.$$

By DeMorgan's laws, we obtain $ab' + a'b < x$. This, together with the previous result $ab' + a'b > x$, implies $x = ab' + a'b$. This completes the proof.[1]

By defining $0 * a = a'$, $0 * a' = a$, $0 * I = I$, $I * a = a$, $I * a' = a'$, and $a * a' = I$ in the Boolean algebra of four elements 0, I, a, a', we obtain an example which shows that a metric quasigroup operation in a Boolean algebra need not be the symmetric difference.

3. Boolean operations. Bernstein [**1**] has characterized Boolean group operations using a definition of a group which differs somewhat from the one now in use in that he did not require that the law of unique solution hold. I am indebted to Professor B. M. Stewart for pertinent observations which led to the following theorem. This theorem is similar to those in [**1**].

[1]The referee observes that we need only have assumed a one-sided loop. Indeed, it is also true that no use was made of the uniqueness of the solution.

https://doi.org/10.4153/CJM-1953-037-7 Published online by Cambridge University Press

THEOREM 3.1. *Any Boolean group operation in a Boolean algebra is an abelian group operation, and is of the form*

$$x * y = e(xy + x'y') + e'(xy' + x'y)$$

where e is the group identity.

Proof. Since the operation $*$ is Boolean, we may write

$$x * y = Axy + Bxy' + Cx'y + Dx'y'$$

where A, B, C, and D are elements of the Boolean algebra (cf. [**1**]). We first note that $0 * D = CD$, and that $0 * C' = DC$, hence $D = C'$ by the law of unique solution. Now $D * 0 = BD$ and $B' * 0 = DB$ implies $D = B'$ by the law of unique solution. Let us designate the identity element of the group by e. We then have $e * e' = e'$ by group properties, but from our original relation we find that $e * e' = B$, hence $B = e'$. Since

$$e = e * e = Ae + De' = Ae + B'e' = Ae + ee' = Ae,$$

we have that $B' = AB'$. Now

$$A' * B = B(A'B' + AB) + B'AB' = AB + AB' = A,$$

and

$$B * B = ABB + B(BB' + B'B) + B' = AB + B' = AB + AB'.$$

Thus $B * B = A$, and $A = B'$ by the law of unique solution. Since $A = B' = D = e$, and $B = D' = C = e'$, we may write

$$x * y = e(xy + x'y') + e'(xy' + x'y).$$

The fact that $x * y = y * x$ is obvious, since the right-hand side of the above expression is symmetric in x and y.

COROLLARY. *The only Boolean group operation in a Boolean algebra with* 0 *as the identity is the symmetric difference.*

This result may be weakened slightly to yield

THEOREM 3.2. *The only Boolean group operation in a Boolean algebra such that* $0 * 0 = 0$ *is the symmetric difference.*

Proof. From $x * y = e(xy + x'y') + e'(xy' + x'y)$ we obtain

$$0 = 0 * 0 = eII = e.$$

Noticing that no use was made of the associative law in the proof of Theorem 3.1, we obtain another theorem.

THEOREM 3.3. *Any Boolean loop operation in a Boolean algebra is an abelian group operation and is of the form*

$$x * y = e(xy + x'y') + e'(xy' + x'y),$$

where e is the loop identity.

https://doi.org/10.4153/CJM-1953-037-7 Published online by Cambridge University Press

Proof. The fact that the operation is of this form and is abelian is proved exactly as in Theorem 3.1. We first show that the associative law holds. Using the definition of $*$, it can be shown in a straightforward manner that

$$z*(x*y) = xyz + x'y'z + xy'z' + x'yz'$$

and that

$$(z*x)*y = xyz + x'y'z + xy'z' + x'yz'.$$

Now, since an associative loop is a group, the theorem follows.

COROLLARY. *The only Boolean loop operation in a Boolean algebra with* 0 *as the loop identity is the symmetric difference.*

THEOREM 3.5. *The only Boolean loop operation in a Boolean algebra such that* $0*0 = 0$ *is the symmetric difference.*

Proof. As is Theorem 3.2, it is easy to show that $e = 0$.

DEFINITION. A binary operation is called *semi-metric* if it satisfies M1 and M2.

THEOREM 3.6. *The only Boolean semi-metric operation in a Boolean algebra is the symmetric difference.*

Proof. Since the operation is Boolean, according to Bernstein [**1**] it is of the form

$$x*y = (I*I)xy + (I*0)xy' + (0*I)x'y + (0*0)x'y'.$$

But since the operation is also semi-metric, we have that

$$I*I = 0*0 = 0, \text{ and } 0*I = I*0.$$

Let $0*I = X$. We can determine X by noting that

$$I*X = X(IX' + I'X) = XX' = 0.$$

Therefore $I = X$ by M1, and the theorem is proved.

4. Other characterizations. Frink [**5**] has characterized the symmetric difference as the only Boolean group operation over which the meet distributes. In this section we will not restrict ourselves to Boolean operations.

THEOREM 4.1. *The only semi-metric group operation in a Boolean algebra over which the meet distributes is the symmetric difference.*

Proof. It can be shown that 0 is the group identity. If a, b, and c are sides of the triangle l, m, n, then $a*b = c$, $b*c = a$, and $a*c = b$. This follows from the associative law and M1, for

$$a*b = (l*m)*(m*n) = l*(0*n) = l*n = c$$

https://doi.org/10.4153/CJM-1953-037-7 Published online by Cambridge University Press

and similarly for the other two cases. We now show that the sum of any two sides of our triangle is over the third.

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

Hence $(a+b)c = c$, so $a+b > c$, which shows that the triangle inequality holds. Thus $*$ is a metric group operation, and is the symmetric difference by Theorem 2.1.

The following example shows that there are semi-metric group operations over which the meet does not distribute. In the Boolean algebra of eight elements, we define an operation $*$ by the following operation table:

$*$	0	a	b	c	a'	b'	c'	I
0	0	a	b	c	a'	b'	c'	I
a	a	0	b'	c'	I	b	c	a'
b	b	b'	0	a'	c	a	I	c'
c	c	c'	a'	0	b	I	a	b'
a'	a'	I	c	b	0	c'	b'	a
b'	b'	b	a	I	c'	0	a'	c
c'	c'	c	I	a	b'	a'	0	b
I	I	a'	c'	b'	a.	c	b	0

Here $*$ is a semi-metric group operation, but

$$a'(c*a) = a'c' = b$$

while

$$a'c * a'a = c*0 = c.$$

THEOREM 4.2. *The only semi-metric semi-group operation in a Boolean algebra over which the meet distributes is the symmetric difference.*

Proof. If $a = b*c$, then $a*b = c$. For

$$0 = a*(b*c) = (a*b)*c$$

by the associative law, whence $a*b = c$ by M1. Thus $0*a = a$, for if $0*a = b$, then $0 = a*b$ implies $a = b$. Now we show that the operation is metric exactly as in Theorem 4.1, and Theorem 2.2 tells us that $*$ is the symmetric difference.

THEOREM 4.3. *The only semi-metric weakly associative operation in a Boolean algebra over which the meet distributes is the symmetric difference.*

Proof. Since $a*a = 0$, it follows that

$$0 = 0*(a*a) = (0*a)*a.$$

Thus $a = 0*a$ by M1. We prove that $*$ is metric as in Theorem 4.1, and apply Theorem 2.3 to complete the proof.

https://doi.org/10.4153/CJM-1953-037-7 Published online by Cambridge University Press

DEFINITION. Let $\circ$ denote the symmetric difference. A binary operation $*$ is said to be *quasi-analytical* [8] when $(a*b) \circ (c*d) < a\circ c + b\circ d$ for all quadruples a, b, c, d of a Boolean algebra.

THEOREM 4.4 (Marczewski). *The only quasi-analytical group operation in a Boolean algebra with 0 as the group identity is the symmetric difference.*

Proof. We will show first that $a = a^{-1}$.

$$a = a\circ 0 = (a*0)\circ(a*a^{-1}) < a\circ a + 0\circ a^{-1} = a^{-1},$$

$$a^{-1} = a^{-1}*0 = (a^{-1}*0)\circ(a^{-1}*a) < a^{-1}\circ a^{-1} + 0\circ a = a.$$

Hence $a > a^{-1}$ and $a < a^{-1}$, which implies that $a = a^{-1}$.

Now $a*b = 0$ if and only if $a = b$. For, let $a = b$. Then $a*a = a*a^{-1} = 0$. Let $a*b = 0$. Then $a*a^{-1} = 0$ implies $b = a^{-1} = a$ by the law of unique solution. This proves M1. To prove M2, we write

$$(a*b)*(b*a) = a*(b*(b*a)) = a*((b*b)*a)$$
$$= a*(0*a) = a*a = 0.$$

Hence $a*b = b*a$ by M1.

To prove M3, let a, b, and c be sides of the triangle l, m, n with $a = l*m$, $b = m*n$, and $c = l*n$. Then

$$a*b = (l*m)*(m*n) = l*n = c.$$

Similarly $a = b*c$ and $b = a*c$. Now

$$c = a*b = (0*0)\circ(a*b) < 0\circ a + 0\circ b = a + b.$$

Thus M3 is proved, and $*$ is a metric group operation in a Boolean algebra. Hence $*$ is the symmetric difference by Theorem 2.1.

In Marczewski's proof, he shows first that the operation $*$ is Boolean. It then follows from Theorem 3.1 or Bernstein's results [**1**] that the operation is the symmetric difference.

5. Concluding remarks. Many of the foregoing results concerning Boolean algebras with metric operations are valid, with obvious modifications, in a generalized Boolean algebra, i.e., in a relatively complemented distributive lattice with 0. Thus Theorem 2.1 could read:

THEOREM. *The only metric group operation in a generalized Boolean algebra is the "relative symmetric difference."*

It would be interesting to know which lattices admit metric group operations. It is easy to construct examples of non-distributive modular lattices and non-modular lattices which admit such operations. However, it has been shown that the only distributive lattices satisfying the descending chain condition

https://doi.org/10.4153/CJM-1953-037-7 Published online by Cambridge University Press

which admit metric group operations are the Boolean algebras.[2] Thus, for example, the only finite distributive lattices admitting such operations are the finite Boolean algebras. Efforts are in progress to extend this result to all distributive lattices. Detailed proofs of the above remarks will be found in the author's thesis.

Finally, it has recently come to our attention that our Theorem 2.1 has been in essence established by Gleason [**6**] in a note extending the work of Helson [**7**].

[2]This result is due to L. M. Kelly.

References

1. B. A. Bernstein, *Operations with respect to which the elements of a Boolean algebra form a group*, Trans. Amer. Math. Soc., *26* (1924), 171–175.
2. ———, *On the existence of fields in Boolean algebras*, Trans. Amer. Math. Soc., *34* (1928), 654–657.
3. D. Ellis, *Autometrized Boolean algebras* I, Can. J. Math., *3* (1951), 87–93.
4. ———, *Geometry in abstract distance spaces* (Debrecen, Hungary, 1951), 3.
5. O. Frink, *On the existence of linear algebras in Boolean algebras*, Bull. Amer. Math. Soc., *34* (1928), 329–333.
6. A. M. Gleason, *A note on a theorem of Helson*, Colloquium Mathematicum, *2* (1949), 5–6.
7. H. Helson, *On the symmetric difference of sets as a group operator*, Colloquium Mathematicum, *1* (1948), 203–205.
8. E. Marczewski, *Concerning the symmetric difference in the theory of sets and in Boolean algebras*, Colloquium Mathematicum, *1* (1948), 199–202.

Michigan State College