Journal of the Mathematical Society of Japan Vol. 5, Nos. 3~4, November, 1953.

Remarks on Boolean functions.[1]

David ELLIS *in Gainesville, Florida*

(Received April 28, 1953)

1. Introduction. Let B be a Boolean algebra with partial ordering, meet, join, complement, and symmetric difference denoted by $a\leqslant b$, $a\wedge b$, $a\vee b$, a', and $a\oplus b$, respectively. When employing the ring notation (11), in B we write merely ab for $a\wedge b$.

Numerous authors have considered Boolean functions [1, 6, 7, 8, 9, 10] of one or more variables. In this note we restrict attention for the most part to Boolean functions of one variable. As is well known [1, 6], every such function allows representation in its disjunctive normal form

$$(卍)\quad f(x)=(a\wedge x)\vee(b\wedge x'),$$

or, in ring notation, $f(x)=(a\oplus b)x\oplus b$.

It is clear that (卍) is a motion of B as an autometrized Boolean algebra [2, 3] if and only if $a=b'$. We shall need the following two lemmas.

LEMMA 1. (*Solution Criterion* [1]). *The equation $ax=b$ has solutions in B if and only if $ab=b$ in which case the general solution is $x=b\oplus t;\ t\leqslant 1\oplus a$.*

LEMMA 2. (*Müller's Theorem* [9, 10]). *The function* (卍) *maps B onto $[a\wedge b,\ a\vee b]$.*

COROLLARY. *The function* (卍) *takes on minimum and maximum values $a\wedge b$ and $a\vee b$, respectively.*

From Lemma 2 one may observe with Schmidt [10] that $a=b'$ is necessary in order that (卍) map B onto itself.

Combining this last remark with the remark preceding Lemma 1, we have

LEMMA 3. *The Boolean functions which map B onto itself are the autometrized motions of B and, hence, are necessarily biuniform.*

1) Presented to the American Mathematical Society; Christmas, 1952.

Since the class of Boolean functions in B is precisely the class of linear functions in ring notation, and since a transformation product of linear functions (possibly constant) is a linear function in a ring, the class of Boolean functions in B is closed under transformation product.

2. The operator structure of the class of Boolean functions. From Lemma 3 and the remark following it in Section 1, we may conclude

THEOREM 1. *The class of Boolean functions on B forms a transformation semigroup on B in which the group of units is precisely the group of motions of B in its autometrization, or, equivalently, the regular representation of the additive group of B under* $(+)$ (see [2, 3, 5]).

THEOREM 2. *The class R of Boolean functions on B forms an operator ring on B. The constant functions form an ideal* J_c *in R and* R/J_c *is a Boolean ring with identity isomorphic to B.*

PROOF. One easily verifies the distributive laws for transformation product over symmetric difference. This proves the first statement. That J_c is an ideal is also easily verified, and the required isomorphism is $a \leftrightarrows \{ax\}$, where $\{ax\}$ is the congruence class of the function mod J_c.

3. Müller's Theorem.

THEOREM 3. *The minimum arguments for which* (⊤) *takes on its minimum and maximum values, respectively, are* $a' \wedge b$ *and* $a \wedge b'$. *The maximum arguments for which* (⊤) *takes on its minimum and maximum values, respectively, are* $a' \vee b$ *and* $a \vee b'$.

PROOF. Suppose $(a \wedge x) \vee (b \wedge x') = a \wedge b$. Then $a' \wedge b \wedge x' = 0$ so that $a' \wedge b \leqslant x$. Also,

$$\big(a \wedge (a' \wedge b)\big) \vee \big(b \wedge (a' \wedge b)'\big) = a \wedge b. \text{ Similarly,}$$

$$\big(a \wedge (a \wedge b')\big) \vee \big(b \wedge (a \wedge b')'\big) = a \vee b \text{ and}$$

$$(a \wedge x) \vee (b \wedge x') = a \wedge b \text{ implies } a \wedge b' \wedge x = a \wedge b'$$

so that $a \wedge b' \leqslant x$. The second part of Theorem 3 follows dually.

We may generalize Müller's theorem to Boolean functions of several variables by induction. Let $f(x_1, x_2, \cdots, x_{n-1}, x_n)$ be a Boolean function of n variables. We may write it in the disjunctive normal form as

$$(\ddagger\ \ddagger)\ f(x_1,\cdots,x_n)=\bigvee_{P_i}\left\{a_i\wedge\left[\bigwedge_{j=1}^{n}x_j^i\right]\right\},$$

where x_j^i is either x_j or x_j' and P_i ranges over the various combinations of these choices.

THEOREM 4. *The function* (‡ ‡) *maps* B^n *onto* $\left[\bigwedge_{P_i} a_i, \bigvee_{P_i} a_i\right]$.

PROOF. The proposition is valid for $n=1$, by Müller's theorem. Suppose it is valid for all $k<n$. Write (‡ ‡) as $f(x_1,\cdots,x_{n-1},x_n)$ $=\bigvee_{P_i}\left\{\left[(a_i\wedge x_n)\vee(b_i\wedge x_n')\right]\wedge\left[\bigwedge_{j=1}^{n-1}x_j^i\right]\right\}$. Where the b_i are the a_i corresponding to values of P_i for which x_n^i is x_n'.

For each value of x_n, (‡ ‡) maps B^{n-1} onto

$$\left[\bigwedge_{P_i}\left\{(a_i\wedge x_n)\vee(b_i\wedge x_n')\right\},\ \bigwedge_{P_i}\left\{(a_i\wedge x_n)\vee(b_i\wedge x_n')\right\}\right]$$

by the inductive hypothesis. We may rewrite this interval as $[(a\wedge x_n)\vee(b\wedge x_n'),\ (c\wedge x_n)\vee(d\wedge x_n')]$, where $a=\bigwedge_{P_i}a_i$, $b=\bigwedge_{P_i}b_i$, $c=\bigvee_{P_i}a_i$, $d=\bigvee_{P_i}b_i$. By Müller's theorem, however, a suitable choice of x_n will lower the left endpoint of the interval to $a\wedge b$ and another choice will raise the right endpoint to $c\vee d$.

We now observe an interesting application of Müller's theorem. It is well-known [1] that in a normed lattice, the triangle function $\delta(x)=\delta(a,x)+\delta(b,x)+\delta(c,x)$ takes on a minimum at $x=(a,b,c)$, the "median" of the triangle [1]. Our application is to obtain the corresponding fact for the triangle function $d(x)=d(a,x)\cup d(b,x)\cup d(c,x)$ in the autometrization of B.

THEOREM 5. $d(x)$ *takes its minimum value at* $x=(a,b,c)$.

PROOF. Since $d(x)=[(a'\vee b'\vee c')\wedge x]\vee[(a\vee b\vee c)\wedge x']$, the minimum values is, by the Corollary to Müller's theorem, $(a'\vee b'\vee c')\wedge(a\vee b\vee c)$. But one verifies by direct computation that this is $d((a,b,c))$. One might also observe that this value is the "perimeter" of the triangle, $d(a,b)\vee d(b,c)\vee d(a,c)$.

4. Curve fitting. In a 1936 paper [8] J.C.C. McKinsey discusses the fitting of graphs of Boolean function of n variables to sets of points in B^{n+1}. His results are, however, qualitative. In this section we determine the exact families of Boolean function of a single variable whose graphs pass through one or a pair of preassigned points in B^2.

In addition to the case of exact fit, we also discuss the curve of best fit to a set of points in B^2 in the following sense: If (x_i, y_i); $i=1, 2, \cdots, n$ is a finite set of points in B^2, and if $f(x)=y$ is a Boolean function in B, then by the total deviation of the function from the set we shall mean $\bigvee_{i=1}^{n}\left(y_i \oplus f(x_i)\right)$; that is, the join of the autometrized distances between actual ordinates and computed ordinates. The curve (or, more precisely, a curve) of best fit will be one whose total deviation from the set is minimal. Obviously, a curve will be an exact fit if and only if the total deviation is 0.

THEOREM 6. *If (x_1, y_1) is any point in B^2, there is a two-parameter family (possibly degenerate) of Boolean functions whose graphs pass through (x_1, y_1), namely,*

$$f_{s,t}(x)=\left(y_1(1 \oplus x_1) \oplus s \oplus t\right) x \oplus y_1 \oplus s; \text{ where } s \leqslant x_1 \text{ and } t \leqslant 1 \oplus x_1 .$$

PROOF. The statement is verified by direct computation.

THEOREM 7. *Let (x_1, y_1) and (x_2, y_2) be any pair of points in B^2. There is a Boolean function whose graph passes through the pair if and only if $y_1 \oplus y_2 \leqslant x_1 \oplus x_2$ in which case there is a one-parameter (possibly degenerate) family of such functions, namely,*

$$f_t(x)=\left((y_1 \oplus y_2) \oplus t\right) x \oplus \left(y_1 \oplus x_1(y_1 \oplus y_2) \oplus x_1 t\right); \text{ where } t \leqslant 1 \oplus x_1 \oplus x_2 .$$

PROOF. $f_t(x)$ as given goes through (x_1, y_1) by Theorem 6. By Lemma 1, one finds that $f_t(x_2)$ is y_2 if and only if the conditions given in Theorem 7 are valid.

THEOREM 8. *A Boolean curve of best fit, $f(x)=(a \oplus b)x \oplus b$, with respect to the set (x_i, y_i); $i=1, \cdots, n$, is obtained by taking*

$$a=\left[\left(\bigwedge_{i=1}^{n} y_i\right) \wedge \left(\bigvee_{i=1}^{n}(x_i \oplus y_i)'\right) \wedge \left(\bigvee_{i=1}^{n}(x_i \oplus y_i)\right)\right] \vee \left[\left(\bigvee_{i=1}^{n} y_i'\right) \wedge \left(\bigwedge_{i=1}^{n}(x_i \oplus y_i)'\right) \wedge \left(\bigvee_{i=1}^{n} y_i\right)\right] \text{ and } b=\left[\left(\bigwedge_{i=1}^{n} y_i\right) \wedge \left(\bigvee_{i=1}^{n}(x_i \oplus y_i)\right)\right] \vee \left[\left(\bigwedge_{i=1}^{n}(x_i \oplus y_i)\right) \wedge \left(\bigvee_{i=1}^{n} y_i\right)\right].$$

In this case, the total deviation will be

$$\left(\bigvee_{i=1}^{n} y_i'\right) \wedge \left(\bigvee_{i=1}^{n}(x_i \oplus y_i)'\right) \wedge \left(\bigvee_{i=1}^{n}(x_i \oplus y_i)\right) \wedge \left(\bigvee_{i=1}^{n} y_i\right).$$

PROOF. To verify Theorem 8, one merely regards the total deviation of an arbitrary curve with respect to the given set of points as a Boolean function of the coefficients and applies Theorem 4.

5. The special case. Homomorphism and orbital topologies. In this section, we restrict attention to those functions (†) for which $b \leqslant a$. By Lemma 2, such a function maps B onto $[b, a]$. This case we call the special case. For the notions involved in the discussion of orbital topologies, see [4]. We denote by B_f the space of B under the orbital topology induced by $f(x)$.

THEOREM 9. *For the special case, $f\big(f(x)\big)=f(x)$; for all x. Also, $f(x)=f(y)$ if and only if $x=y \pmod{J_f}$, where J_f is the principal ideal of $1 \oplus a \oplus b$.*

PROOF. The first assertion follows by direct computation. Suppose $x \oplus y \leqslant 1 \oplus a \oplus b$. Then $f(x) \oplus f(y)=(a \oplus b)(x \oplus y) \oplus b \oplus b=0$. Conversely, if $f(x) \oplus f(y)=0$, then $(a \oplus b)(x \oplus y)=0$ and $x \oplus y \leqslant 1 \oplus a \oplus b$.

THEOREM 10. *For the special case, $f(x)$ is a lattice homomorphism of B onto $[b, a]$ and, in B_f, x is an accumulation point of a set E if and only if x is in $[b, a]$ and E contains infinitely many points of the congruence class of x $\bmod J_f$.*

PROOF. In the special case, $(a \oplus b)b=0$. Thus, $f(u \vee v)=(a \oplus b)(u \oplus v \oplus uv) \oplus b$ and $f(u) \vee f(v)=(a \oplus b)(u \oplus v \oplus uv) \oplus b \oplus (a \oplus b) b(u \oplus v)$ $f(u \vee v) \oplus 0$. Similarly, $f(u \vee v)=f(u) \wedge f(v)$. This proves the first assertion. If $f(y)=x$, then $(a \oplus b)y=x \oplus b$, $(a \oplus b \oplus 1)y=(x \oplus y) \oplus b$, $x \oplus y =(a \oplus b \oplus 1)y \oplus b$. But, $(a \oplus b \oplus 1)y$ is in J_f and, in the special case, $b=b(a \oplus b \oplus 1)$ is in J_f so that $x=y \pmod{J_f}$.

THEOREM 11. *In the special case, I, the principal ideal of $a \oplus b$, is a group of homoemorphisms of B_f onto itself.*

PROOF. Take c in I and consider T_c, the $\oplus$ translation by c. $f(x \oplus c)=(a \oplus b)(x \oplus c) \oplus b=(a \oplus b)x \oplus b \oplus c$, since c is in I. Hence, $f(xT_c)=\big(f(x)\big) T_c$ and T_c commutes with f. Also, T_c is biuniform and is its own inverse so that T_c is a homeomorphism of B_f onto itself by Theorem 5 of [4].

THEOREM 12. *In the lattice of all topologies on B, the join of the orbital topologies induced by functions in the special case is the strongest T_1 topology on B* (see [12] for terminology).

PROOF. Taking $a=b$ in $f(x)$ we find $J_f=B$. By Theorem 10, then, only finite sets are closed in the join of these topologies.

The University of Florida

Bibliography

[1] Garrett Birkhoff, *Lattice Theory* (*Revised Edition*), American Mathematical Society, 1948, New York.
[2] David Ellis, *Autometrized Boolean algebras I*, Canadian Jour. of Math. vol. 3 (1951), pp. 87-93.
[3] David Ellis, *Autometrized Boolean algebras II*, Canadian Jour. of Math., vol. 3 (1951), pp. 145-147.
[4] David Ellis, *Orbital topologies*, To appear in Quart. Jour. of Math. (Oxford), early 1953.
[5] N. Jacobson, *Lectures in Abstract Algebra*, Van Nostrand, 1951, New York.
[6] S. A. Kiss, *Structures of Logic*, Stephen A. Kiss, 1947, New York.
[7] J. C. C. McKinsey, *On Boolean functions of many variables*, Trans. Am. Math. Soc., vol. 40 (1936), pp. 343-362.
[8] J. C. C. McKinsey, *Boolean functions and points*, Duke Math. Jour., vol. 2 (1936), pp. 465-471.
[9] Eugen Müller, *Schröder's Abriss der Algebra der Logik*, 1909, Leipzig.
[10] Karl Schmidt, *The theory of functions of one Boolean variable*, Trans. Am. Math. Soc., vol. 23 (1922), pp. 212-222.
[11] M. H. Stone, *Subsumption of Boolean algebra under the general theory of rings*, Proc. Nat. Acad. Sci., vol. 20 (1934), pp. 197-202.
[12] R. Varidyanathaswami, *Treatise on Set Topology*, Indian Math. Soc.. 1947, Madras.