Journal of the Mathematical Society of Japan Vol. 8 No. 4, October, 1956

Remarks on Boolean functions II.[1]

By David ELLIS

(Received April 6, 1956)

1. Introduction.

This paper continues our remarks on Boolean functions [7][2]. In the present paper we are concerned with the groupoids [5] arising from functions of two variables and with the factorization of general functions. Some of the matters in Sections 3 and 4 have been partially discussed previously in [3] and [9], respectively. The Boolean algebra, B, considered throughout is strictly arbitrary.

2. Preliminaries.

Let B be a Boolean algebra [1] with meet, join, and complement indicated by $x\wedge y, x\vee y$, and x^{*}, respectively. We shall also employ the ring notation [10], $x+y$ and xy, where these denote sum and product, respectively. One recalls [10]:

$$x+y=(x\wedge y^{*})\vee(x^{*}\wedge y)$$
$$xy=x\wedge y$$
$$x\vee y=x+y+xy\,.$$

The first and last elements of B (additive and multiplicative identities in the ring) will be denoted by 0 and 1, respectively.

One recalls [1] that any Boolean function, $f(x,y)$, of two variables over B may be written in its disjunctive normal form:

$$(\dagger)\ f(x,y)=(a\wedge x\wedge y)\vee(b\wedge x\wedge y^{*})\vee(c\wedge x^{*}\wedge y)\vee(d\wedge x^{*}\wedge y^{*})\,.$$

The standard ring form of $f(x,y)$ is

1) Presented to the Mathematical Association of America, Athens, Georgia, March 1956.
2). Numbers in square brackets refer to the list of references concluding the paper.

$$(\dagger\dagger)\ f(x, y) = \alpha xy + \beta x + \gamma y + \delta\,.$$

We refer to either (†) or (††) as the canonical form of $f(x, y)$ and the two are related by the following equalities among constants:

$$\begin{aligned} a+b+c+d &= \alpha \qquad & \alpha+\beta+\gamma+\delta &= a \\ b+d &= \beta & \beta+\delta &= b \\ c+d &= \gamma & \gamma+\delta &= c \\ d &= \delta & \delta &= d \end{aligned}$$

3. The semigroups and quasigroups.

LEMMA 1. *A Boolean function $f(x, y) = \alpha xy + \beta x + \gamma y + \delta$ yields a semigroup* [5] *in B if and only if $\alpha\gamma = \alpha\beta$, $\delta\gamma = \delta\beta$, and $\alpha\delta = 0$.*

PROOF. These are precisely the conditions for $f(x, f(y, z)) = f(f(x, y), z)$ to be an identity as may be verified by direct computation.

LEMMA 2. *A Boolean function $f(x, y) = \alpha xy + \beta x + \gamma y + \delta$ yields an Abelian groupoid* [5] *in B if and only if $\beta = \gamma$.*

PROOF. Obvious.

LEMMA 3. *A Boolean function $f(x, y) = \alpha xy + \beta x + \gamma y + \delta$ yields a quasigroup* [5] *in B if and only if $\alpha = 0$ and $\beta = \gamma = 1$.*

PROOF. $f(x, y)$ yields a quasigroup if and only if $f(a, x)$ and $f(x, a)$ are permutations of B for each $a \in B$.

$$f(a, x) = (\alpha a + \gamma)x + (\beta a + \delta) = ((\alpha a + \gamma + \beta a + \delta) \wedge x) \vee ((\beta a + \delta) \wedge x^*)$$

$$f(x, a) = (\alpha a + \beta)x + (\gamma a + \delta) = ((\alpha a + \beta + \gamma a + \delta) \wedge x) \vee ((\gamma a + \delta) \wedge x^*)$$

For these to be mappings of B onto itself we must have, by Müller's Theorem [7],

$$(\alpha a + \gamma + \beta a + \delta) \vee (\beta a + \delta) = 1,\ (\alpha a + \gamma + \beta a + \delta) \wedge (\beta a + \delta) = 0$$

$$(\alpha a + \beta + \gamma a + \delta) \vee (\gamma a + \delta) = 1,\ (\alpha a + \beta + \gamma a + \delta) \wedge (\gamma a + \delta) = 0$$

for all $a \in B$. Combining these and changing to pure ring notation yields

$$\alpha a + \gamma = 1,\ \alpha a + \beta = 1 \quad \text{for all } a \in B\,.$$

Thus, it is necessary that $\beta = \gamma = 1$ and $\alpha = 0$ so that $f(x, y) = x + y + \delta$. This condition is also sufficient since $f(a, x) = (a + \delta) + x = f(x, a)$ is merely a ring translation and, hence, a permutation of B.

THEOREM 1. *The quasigroups arising in B from the Boolean function $f(x,y)$ comprise the one-parameter family $f(x,y)=x+y+\delta$ and are actually Abelian groups of nilpotents.*

PROOF. From Lemmas 1, 2 and 3, we see that $f(x,y)=x+y+\delta$ yields an Abelian semigroup which is also a quasigroup and, hence, a group [2]. Since $f(x,\delta)=f(\delta,x)=x$, δ is the identity of the group and since $f(x,x)=\delta$, each element is nilpotent.

4. Semilattices and symmetries of *B*.

LEMMA 4. *A Boolean function $f(x,y)=\alpha xy+\beta x+\gamma y+\delta$ yields a groupoid of idempotents* [4] *if and only if $\alpha+\beta+\gamma=1$ and $\delta=0$.*

PROOF. The requirement is $f(x,x)=\alpha x+\beta x+\gamma x+\delta=x$ for all $x\in B$. The conclusion follows.

THEOREM 2. *A Boolean function $f(x,y)=\alpha xy+\beta x+\gamma y+\delta$ yields a semilattice* [4] *if and only if $\alpha=1$, $\delta=0$, $\beta=\gamma$.*

PROOF. The proposition is immediate from Lemmas 1, 2 and 4.

THEOREM 3. *The semilattices arising in B from Boolean fnnctions $f(x,y)$ comprise the one-parameter family $xy+\lambda(x+y)$. If one defines $x\underset{\lambda}{\vee}y=xy+\lambda(x+y)$ and $x\underset{\lambda}{\wedge}y=xy+(1+\lambda)(x+y)$ then with $x\underset{\lambda}{\vee}y$ as join and $x\underset{\lambda}{\wedge}y$ as meet and x^* as complement, B forms a Boolean algebra with first element λ^* and last element λ. Thus, for each element, λ, of B there is a Boolean algebra on B having λ as last element, called the λ-algebra. The 1-algebra is, of course, the original algebra and the 0-algebra its dual. For any $\lambda,\mu\in B$, the λ-algebra and μ-algebra are isomorphic and the isomorphism if $f_{\lambda\mu}(x)=f_{\mu\lambda}(x)=x+\mu+\lambda$ which is precisely the motion* [6] *of B taking μ into λ. Thus, motions preserve not only geometry but algebra in B. The transformation equation between λ-algebra and μ-algebra are*

$$x\underset{\lambda}{\vee}y=[\lambda^*\underset{\mu}{\wedge}(x\underset{\mu}{\wedge}y)]\underset{\mu}{\vee}[\lambda\underset{\mu}{\wedge}(x\underset{\mu}{\vee}y)]$$

$$x\underset{\lambda}{\wedge}y=[\lambda\underset{\mu}{\wedge}(x\underset{\mu}{\wedge}y)]\underset{\mu}{\vee}[\lambda^*\underset{\mu}{\wedge}(x\underset{\mu}{\vee}y)]$$

$$x^*=x^*\,.$$

One has the identities

$$(x \underset{\lambda}{\wedge} y) \underset{\mu}{\vee} (x \underset{\lambda}{\vee} y) = x \underset{\mu}{\vee} y$$

$$(x \underset{\lambda}{\wedge} y) \underset{\mu}{\wedge} (x \underset{\lambda}{\vee} y) = x \underset{\mu}{\wedge} y$$

so that all of the semilattices mentioned in Theorem 2 *are c-functions* [8] *in the* μ*-algebra for any* $\mu \in B$. *Finally, the ring addition associated with the* λ*-algebra as symmetric difference is precisely that quasigroup mentioned in Theorem* 1 *whose parameter value is* λ^*. *That is,* $x \underset{\lambda}{+} y = x + y + \lambda^* = x \underset{\mu}{+} y \underset{\mu}{+} \lambda^*$.

PROOF. The first assertion is merely a restatement of Theorem 2. The remaining assertions are proved by straightforward computation. As an example, we show the first part of the last equality, $x \underset{\lambda}{+} y = x + y + \lambda^*$.

$$\begin{aligned}
& x \underset{\lambda}{+} y = (x \underset{\lambda}{\wedge} y^*) \underset{\lambda}{\vee} (x^* \underset{\lambda}{\wedge} y) = \\
& [x(1+y) + (1+\lambda)(x+1+y)] \underset{\lambda}{\vee} [(1+x)y + (1+\lambda)(1+x+y)] = \\
& [x(1+y) + (1+\lambda)(x+1+y)] + [(1+x)y + (1+\lambda)(1+x+y)] + \\
& \lambda[(1+x)y + (1+\lambda)(1+x+y) + x(1+y) + (1+\lambda)(x+1+y)] = \\
& (1+\lambda)(1+x+y) + \lambda(x+y) = x+y+(1+\lambda) = x+y+\lambda^* .
\end{aligned}$$

REMARK. Knowing that any set having 2^n elements may be made into a Boolean algebra, we may apparently conclude that this may be done with any desired involutory permutation as complementation and any desired element as last element.

5. Reducibility criterion.

A Boolean function of any finite number of variables may be written in a canonical form similar to (†) or (††). We say that a Boolean function of $x_1, x_2, \cdots, x_{n-1}, x_n$ is reducible in x_n if it is the product of a Boolean function of x_n and a Boolean function of $x_1, x_2, \cdots, x_{n-1}$. If f is a Boolean function of $x_1, \cdots, x_n$, the x_n-matrix of f is obtained as follows: Write f in the ring canonical form regarding x_n as the "last" variable, and utilizing zero coefficients where necessary to make absent terms present. In column 1 write the coefficients, in order, of terms containing x_n and in column 2 write the coefficients, in order, of other terms. The result is a $2\times 2^{n-1}$ matrix. The matrix is said to be singular if its rank is less than 2. To obtain, for example, the x-matrix of $xyz+kxy+z$, we rewrite: $yzx+oyz+kyx+ozx+oy+z+ox+o$ and obtain

$$\left\|\begin{matrix} 1 & 0 \\ k & 0 \\ 0 & 1 \\ 0 & 0 \end{matrix}\right\|, \quad \text{which is non-singular since} \quad \left|\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}\right| = 1.$$

LEMMA 5. *A Boolean function $f(x, y)=\alpha xy+\beta x+\gamma y+\delta$ is reducible in x if and only if it is reducible in y and it is reducible in y if and only if its y-matrix is singular.*

PROOF. The first assertion is immediate from definition. Suppose now that $f(x, y)=(ax+b)(cy+d)$. Then $\alpha=ac$, $\beta=ad$, $\gamma=bc$, $\delta=bd$ so $\alpha\delta=abcb=\beta\gamma$ and $\left\|\begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix}\right\|$ is singular. If, alternatively, $\left\|\begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix}\right\|$ is singular so that $\alpha\delta=\beta\gamma$ one may verify by direct computation that $f(x, y)=(ax+b)(cy+d)$ where

$$a=\alpha\vee\beta,\ b=\gamma\vee\delta,\ c=\alpha\vee\gamma,\ d=\beta\vee\delta$$

THEOREM 4. *If $f(x_1,\cdots, x_n, x_{n+1})$ is a Boolean function, it is reducible in x_{n+1} if and only if its x_{n+1}-matrix is singular.*

PROOF. We merely outline the proof. Make the inductive hypothesis for $n<m$ and write the $xm+1$ matrix for $f(x_1,\cdots, x_m, x_{m+1})$. "Suppress" x_1 by considering it constant and find the x_{m+1}-matrix of the result which is a linear matrix function of x_1. Suppressing $x_2,\cdots\cdots, x_m$ in turn we obtain $2m$ matrices the simultaneous singularity of which is equivalent to the singularity of the desired matrix. The induction is anchored at $n=1$ by Lemma 5.

References

[1] Garrett Birkhoff, *Lattice Theory (Revised Edition)*, American Mathematical Society, New York, 1948.

[2] R. H. Bruck, *Some Results in the Theory of Quasigroups*, Transactions of the American Mathematical Society, 55 (1944), pp. 19-52.

[3] J. G. Elliott, *Autometrization and the Symmetric Difference*, Canadian Journal of Mathematics, 5 (1953), pp. 324-331.

[4] David Ellis, *An Algebraic Characterization of Lattices Among Semilattices*, Portugaliae Mathematica, 8 (1949).

[5] —— ——, *Geometry in Abstract Distance Spaces*, Publicationes Mathematicae, 2 (1951), pp. 1-25.

[6] —— ——, *Autometrized Boolean Algebras II*, Canadian Journal of Mathematics, 3 (1951), pp. 145-147.

[7] —— ——, *Remarks on Boolean Functions*, Journal of the Mathematical Society of Japan, 5 (1953), pp. 345-350.

[8] —— ——, *Notes on the Foundations of Lattice Theory II*, Archiv der Mathematik, 4 (1953), pp. 257-260.

[9] Stephen Kiss, *Transformations on Lattices and Structures of Logic*, Stephen Kiss, New York, 1947.

[10] M. H. Stone, *S..bsumption of Boolean Algebras Under the Theory of Rings*, Proceedings of the National Academy of Sciences (USA), 20 (1934), pp. 197-202.