REDUCIBLE BOOLEAN FUNCTIONS

BY J. C. C. McKINSEY

In this note I establish a condition that a Boolean function of n variables, say f, be reducible to a product of two Boolean functions f_1 and f_2, where f involves variables not occurring in f_i; and, similarly, that f be reducible to f_1+f_2, or to $f_1 \circ f_2$, or to $f_1 \Delta f_2$.* These results are of interest in connection with the general theory of Boolean operations, since every Boolean operation can be regarded as a Boolean function.

In order to state my results briefly, I use the symbol $\oplus$, which stands ambiguously for any one of the four operations $\times$, $+$, $\circ$, Δ. Thus each of my theorems really comprises four theorems, which can be obtained from the given theorem by substituting first $\times$ for $\oplus$ throughout, then $+$, then $\circ$, and then Δ. The theorems now follow.

THEOREM 1. *If a Boolean function*

$$f(x_1, \cdots, x_n)$$

be given, then a necessary and sufficient condition that there exist a g and an h, so that

$$f(x_1, \cdots, x_n) = g(x_1, \cdots, x_p) \oplus h(x_q, \cdots, x_n), \qquad (q \leqq p + 1),$$

is that

* The operation $a \circ b$ is defined by $a \circ b = ab' + a'b$; and the operation $a\Delta b$ is defined by $a\Delta b = ab + a'b'$. These operations, which are mutually dual, are associative and commutative, and satisfy the further laws: $(a \circ b)' = a \circ b' = a\Delta b$, $a \circ 1 = a\Delta 0 = a'$, $a \circ a = a\Delta a' = 0$, $a \circ 0 = a\Delta 1 = a$. For a further discussion, see Bernstein's paper, *Postulates for Boolean algebra involving the operation of complete disjunction*, to appear in the Annals of Mathematics. For a detailed treatment of $a \circ b$, see the two papers by M. H. Stone: *Postulates for Boolean algebra and generalized Boolean algebra*, American Journal of Mathematics, vol. 57 (1935), pp. 703–732, and *Subsumption of the theory of Boolean algebras under the theory of rings*, Proceedings of the National Academy of Sciences, vol. 21 (1935), pp. 103–105. Stone writes $a\Delta b$ for what I designate by $a \circ b$, and he does not discuss the relation which I denote by $a\Delta b$.

$$\begin{aligned} f(x_1, \cdots, x_{q-1}, z_q, \cdots, z_p, x_{p+1}, \cdots, x_n) \\ \oplus f(y_1, \cdots, y_{q-1}, z_q, \cdots, z_p, y_{p+1}, \cdots, y_n) \\ = f(x_1, \cdots, x_{q-1}, z_q, \cdots, z_p, y_{p+1}, \cdots, y_n) \\ \oplus f(y_1, \cdots, y_{q-1}, z_q, \cdots, z_p, x_{p+1}, \cdots, x_n) \end{aligned}$$

*identically.**

PROOF. I first prove the theorem for the case that $q=p+1$. To see that the condition is necessary (when $q=p+1$), suppose that there exists a g and an h so that

$$f(x_1, \cdots, x_n) = g(x_1, \cdots, x_p) \oplus h(x_{p+1}, \cdots, x_n). \tag{1}$$

Then

$$\begin{aligned} f(x_1, \cdots, x_n) \oplus f(y_1, \cdots, y_n) \\ = [g(x_1, \cdots, x_p) \oplus h(x_{p+1}, \cdots, x_n)] \\ \oplus [g(y_1, \cdots, y_p) \oplus h(y_{p+1}, \cdots, y_n)] \\ = [g(x_1, \cdots, x_p) \oplus h(y_{p+1}, \cdots, y_n)] \\ \oplus [g(y_1, \cdots, y_p) \oplus h(x_{p+1}, \cdots, x_n)] \\ = f(x_1, \cdots, x_p, y_{p+1}, \cdots, y_n) \\ \oplus f(y_1, \cdots, y_p, x_{p+1}, \cdots, x_n), \end{aligned} \tag{2}$$

as was to be shown.

To show that the condition is sufficient (when $q=p+1$), suppose that $f(x_1, \cdots, x_n)$ is such that (2) holds. We must now distinguish the four cases. If $\oplus = \times$, define

$$g(x_1, \cdots, x_p) = \sum_{z_i=0,1} f(x_1, \cdots, x_p, z_{p+1}, \cdots, z_n),$$

$$h(x_{p+1}, \cdots, x_n) = \sum_{z_i=0,1} f(z_1, \cdots, z_p, x_{p+1}, \cdots, x_n).$$

Then

$$g(x_1, \cdots, x_p)h(x_{p+1}, \cdots, x_n)$$

$$= \left[\sum_{z_i=0,1} f(x_1, \cdots, x_p, z_{p+1} \cdots, z_n) \right]$$

---

* Or, what amounts to the same thing, that the stated condition hold for the x's, y's, z's$=0$, 1. Thus whether the condition is satisfied can be seen directly from the discriminants of f.

$$\left[\sum_{z_i=0,1} f(z_1, \cdots, z_p, x_{p+1}, \cdots, z_n)\right]$$

$$= \sum_{z_i=0,1} f(x_1, \cdots, x_p, z_{p+1}, \cdots, z_n) f(z_1, \cdots, z_p, x_{p+1}, \cdots, x_n)$$

$$= \sum_{z_i=0,1} f(x_1, \cdots, x_n) f(z_1, \cdots, z_n)$$

$$= f(x_1, \cdots, x_n) \sum_{z_i=0,1} f(z_1, \cdots, z_n)$$

$$= f(x_1, \cdots, x_n).$$

If $\oplus = +$, define

$$g(x_1, \cdots, x_p) = \prod_{z_i=0,1} f(x_1, \cdots, x_p, z_{p+1}, \cdots, z_n),$$

$$h(x_{p+1}, \cdots, x_n) = \prod_{z_i=0,1} f(z_1, \cdots, z_p, x_{p+1}, \cdots, x_n),$$

and proceed as above. If $\oplus = \circ$, define

$$g(x_1, \cdots, x_p) = f(0, \cdots, 0) \circ f(x_1, \cdots, x_p, 0, \cdots, 0),$$

$$h(x_{p+1}, \cdots, x_n) = f(0, \cdots, 0, x_{p+1}, \cdots, x_n).$$

Then

$$\begin{aligned} g(x_1, \cdots, x_p) &\circ h(x_{p+1}, \cdots, x_n) \\ &= f(0, \cdots, 0) \circ f(x_1, \cdots, x_p, 0, \cdots, 0) \\ &\quad \circ f(0, \cdots, 0, x_{p+1}, \cdots, x_n) \\ &= f(0, \cdots, 0) \circ f(0, \cdots, 0) \circ f(x_1, \cdots, x_n) \\ &= 0 \circ f(x_1, \cdots, x_n) \\ &= f(x_1, \cdots, x_n). \end{aligned}$$

If $\oplus = \Delta$, define

$$g(x_1, \cdots, x_p) = f(0, \cdots, 0) \Delta f(x_1, \cdots, x_p, 0, \cdots, 0),$$

$$h(x_{p+1}, \cdots, x_n) = f(0, \cdots, 0, x_{p+1}, \cdots, x_n),$$

and proceed as above. This completes the proof of the theorem for the case $q = p+1$.

For the general case, to say that

$$f(x_1, \cdots, x_n) = g(x_1, \cdots, x_p) \oplus h(x_q, \cdots, x_n) \tag{3}$$

holds for every $x_q, \cdots, x_p$ is equivalent to saying it holds for $x_q, \cdots, x_p=0, 1$. Hence saying that (3) holds for every $x_1, \cdots, x_n$ is equivalent to saying that the following equations hold for every $x_1, \cdots, x_{q-1}, x_{p+1}, \cdots, x_n$:

$$
(4)\quad
\begin{aligned}
&f(x_1, \cdots, x_{q-1}, 1, \cdots, 1, x_{p+1}, \cdots, x_n) \\
&\quad = g(x_1, \cdots, x_{q-1}, 1, \cdots, 1) \oplus h(1, \cdots, 1, x_{p+1}, \cdots, x_n), \\
&\quad \vdots \\
&f(x_1, \cdots, x_{q-1}, 0, \cdots, 0, x_{p+1}, \cdots, x_n) \\
&\quad = g(x_1, \cdots, x_{q-1}, 0, \cdots, 0) \oplus h(0, \cdots, 0, x_{p+1}, \cdots, x_n).
\end{aligned}
$$

It will be noticed that each discriminant of $g(x_1, \cdots, x_p)$, and each discriminant of $h(x_q, \cdots, x_n)$, occurs in *just one* of the equations (4). Hence to say that there exists a $g(x_1, \cdots, x_p)$ and an $h(x_q, \cdots, x_n)$ so that (3) holds identically is equivalent to saying that there exist elements $g(1, \cdots, 1, 1, \cdots, 1), \cdots, g(0, \cdots, 0, 1, \cdots, 1), h(1, \cdots, 1, 1, \cdots, 1), \cdots, h(1, \cdots, 1, 0, \cdots, 0)$ so that the first equation of (4) holds identically, and similarly for each of the other equations of (4). Hence, by the first part of the proof, to say that (3) holds identically is equivalent to saying that the following set of equations hold identically:

$$
(5)\quad
\begin{aligned}
&f(x_1, \cdots, x_{q-1}, 1, \cdots, 1, x_{p+1}, \cdots, x_n) \\
&\qquad \oplus f(y_1, \cdots, y_{q-1}, 1, \cdots, 1, y_{p+1}, \cdots, y_n) \\
&\quad = f(x_1, \cdots, x_{q-1}, 1, \cdots, 1, y_{p+1}, \cdots, y_n) \\
&\qquad \oplus f(y_1, \cdots, y_{q-1}, 1, \cdots, 1, x_{p+1}, \cdots, x_n), \\
&\quad \vdots \\
&f(x_1, \cdots, x_{q-1}, 0, \cdots, 0, x_{p+1}, \cdots, x_n) \\
&\qquad \oplus f(y_1, \cdots, y_{q-1}, 0, \cdots, 0, y_{p+1}, \cdots, y_n) \\
&\quad = f(x_1, \cdots, x_{q-1}, 0, \cdots, 0, y_{p+1}, \cdots, y_n) \\
&\qquad \oplus f(y_1, \cdots, y_{q-1}, 0, \cdots, 0, x_{p+1}, \cdots, x_n).
\end{aligned}
$$

But the set (5) is equivalent to the single condition given in the statement of the theorem.

I now give a partial generalization of Theorem 1 to the case where $f(x_1, \cdots, x_n)$ is reducible to a product (or sum, $\cdots$) of *three* functions. The generalization is not complete, in that it covers only the case where no two of the three functions involve a common variable. The proof, which is closely analogous to the first part of the proof of Theorem 1, is omitted.

THEOREM 2. *If a Boolean function* $f(x_1, \cdots, x_n)$ *be given, then a necessary and sufficient condition that there exist functions* g_1, g_2, g_3 *so that*

$$f(x_1, \cdots, x_n) = g_1(x_1, \cdots, x_p) \oplus g_2(x_{p+1}, \cdots, x_q) \oplus g_3(x_{q+1}, \cdots, x_n)$$

is that

$$\begin{aligned} f(x_1, \cdots, x_n) \oplus f(y_1, \cdots, y_n) &= f(x_1, \cdots, x_p, y_{p+1}, \cdots, y_n) \oplus f(y_1, \cdots, y_p, x_{p+1}, \cdots, x_n) \\ &= f(x_1, \cdots, x_q, y_{q+1}, \cdots, y_n) \oplus f(y_1, \cdots, y_q, x_{q+1}, \cdots, x_n) \end{aligned}$$

identically.

From Theorems 1 and 2 we have immediately the following theorem.

THEOREM 3. *If there exist functions* g_1 *and* g_2 *and also functions* g_3 *and* g_4 *so that*

$$f(x_1, \cdots, x_n) = g_1(x_1, \cdots, x_p) \oplus g_2(x_{p+1}, \cdots, x_n),$$

$$f(x_1, \cdots, x_n) = g_3(x_1, \cdots, x_q) \oplus g_4(x_{q+1}, \cdots, x_n), \quad (p < q),$$

then there exist functions k_1, k_2, k_3 *so that*

$$f(x_1, \cdots, x_n) = k_1(x_1, \cdots, x_p) \oplus k_2(x_{p+1}, \cdots, x_q) \oplus k_3(x_{q+1}, \cdots, x_n).$$

Theorems 2 and 3 are readily generalized to the case where we express f as a product (sum, $\cdots$) of any finite number of other functions.

THE UNIVERSITY OF CALIFORNIA