§ Cat   Boolean fns   Sloane

Self-Complementary Symmetry Types of Boolean Functions*

This note is concerned with those Boolean functions (switching functions) that are of the same symmetry type as their binary complements. Such symmetry types are called *self-complementary.*

The Pólya-Slepian enumeration formula for symmetry types is modified to permit one to count the number of such self-complementary symmetry types for an arbitrary number of variables, n. Using the modified formula, this number has been computed for $n=1$, 2, 3, 4, and 5. For $n=1$, 2, and 3, all *neutral* symmetry types (those with 2^{n-1} "true" entries in the truth table) are self-complementary. When n is greater than three, this relation breaks down and the self-complementary types become increasingly rare.

A network interpretation is given of Slepian's classification of variable transformations into *e-cycles* and *o-cycles* which sheds light on the problem of classifying Boolean functions and relates this problem to sequential network theory.

Boolean functions, $f(x_1 \cdots x_n)$ and $g(x_1 \cdots x_n)$, are said to belong to the same symmetry type if there exists some variable transformation (permutation and/or complementation of some or all of the variables, $x_1, \cdots, x_n$) which changes f into g. Tables[1,2] of symmetry types exist through $n=4$ and the numbers of distinct symmetry types have been calculated[3] up to $n=6$.

Suppose that $f=f(x_1 \cdots x_n)$ is a Boolean function of n variables and that $\bar{f}=\bar{f}(x_1 \cdots x_n)$ is its binary complement. In order for f and $\bar{f}$ to belong to the same symmetry type, it is clearly necessary that f (and, hence, also $\bar{f}$) have value *1* for 2^{n-1} of the 2^n possible input combinations, and have value *0* for the other 2^{n-1} combinations. Such functions (having equal occurrences of value *1* and value *0*) have been called *neutral*[4] and they have important properties in relation to the study of sequential networks.[4]

Consideration of the possible symmetry types of neutral functions readily shows that for $n=1$, 2, and 3, all neutral functions belong to the same symmetry type as their respective binary complements, and, hence are self-complementary. The familiar parity functions are all of this type. Other examples of self-complementary symmetry types are shown in Fig. 1. It should not be thought, however, that neutral symmetry types are invariably self-complementary. Of the 74 neutral symmetry types in four variables, 42 turn out to be self-complementary while the remaining 32 occur in complementary pairs (see Higgonet and Grea[2]). Examples

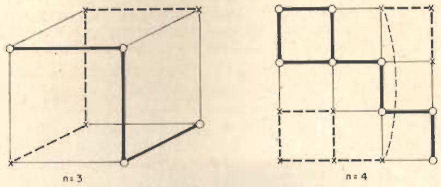

Fig. 1—Examples of self-complementary neutral symmetry types.

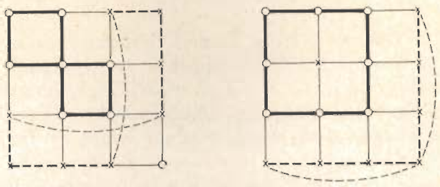

Fig. 2—Karnaugh diagrams of some non-self-complementary neutral symmetry types; $n=4$.

are shown in Fig. 2 by means of Karnaugh diagrams.[5]

The question thus arises as to what happens for $n>4$. How does the class of neutral functions divide into self-complementary (SC) and non-self-complementary (NSC) types? Do both SC and NSC types exist for all values of $n \geq 4$? These questions have been partially answered by an extension of Slepian's methods.[3]

The basic tool in this investigation is the formula (Pólya,[6] Slepian[3])

$$N_n = \frac{1}{n!2^n} \sum_C n_C 2^{K(C)} \qquad (1)$$

for the number of distinct symmetry types of Boolean functions in n (or fewer) variables. Here the summation is extended over all classes C of equivalent operations (variable transformations), with n_C the number of operations in class C while $K(C)$ is the number of cycles into which the vertices of the n-dimensional hypercube are permuted by an operation of class C. Thus, $2^{K(C)}$ gives the number of Boolean functions invariant under an operation of class C. For a more detailed explanation of these concepts, the reader should refer to Slepian's paper.[3]

As pointed out by Golomb,[7] (1) is an instance of a very general expression for the number of transitivity sets into which a space S is decomposed by the operations of a finite transformation group G acting on the points of this space. Two points, s and s', are in the same transitivity set if, and only if, some operation t of G transforms s into s', *i.e.*, if $t(s)=s'$. Let $I(t)$ be the number of points of S which are left fixed by operation t of the group G. Then, the number of transitivity sets is given by

$$N = \frac{1}{n(G)} \sum_{t \in G} I(t) \qquad (2)$$

where $n(G)$ is the order of the group G.

In Slepian's application of this formula, S is the set of all 2^{2^n} n-variable Boolean functions, G is the n-dimensional hypercube group of order $n!2^n$, and the transitivity sets are the symmetry-type classes of Boolean functions. The summation in (1) is carried out, not element by element [as in (2)], but in terms of classes of equivalent, *i.e.*, conjugate,[8] operations. All operations of a given conjugacy class C have similar properties. In particular, they have the same value of $I(t)=2^{K(C)}$.

In order to determine the number of self-complementary neutral types in n variables, let S be the space consisting of all (unordered) pairs $(f, \bar{f})$ of complementary functions of n variables. There are obviously 2^{2^n-1} such pairs. The group G of variable transformations is, as before, the hypercube group of order $n!2^n$, consisting of all permutations and/or complementations of variables. One may define two pairs, $(f, \bar{f})$ and $(g, \bar{g})$, in S to be equivalent under G if some operation in G transforms f into either g or $\bar{g}$. This relation between pairs, which is readily seen to be an equivalance relation (*i.e.*, reflexive, symmetric and transitive) then partitions S into classes of equivalent pairs. These classes of pairs will be referred to as *pair symmetry types*. Thus, pair $(f, \bar{f})$ is of the same pair symmetry type as $(g, \bar{g})$ if, and only if, f is of the same (ordinary) symmetry type as either g or $\bar{g}$. For example, the pair consisting of the even parity and odd parity functions forms a pair symmetry type with only one member. Likewise, the pair (f_0, f_I), where $f_0 \equiv 0$ and $f_I \equiv 1$, also forms such a class. Most pair classes, however, will contain several distinct pairs.

Let $N_n^{(sc)}$ and $N_n^{(nsc)}$ be the numbers of SC and NSC symmetry types, respectively, of n-variable Boolean functions. The SC types form $N_n^{(sc)}$ pair symmetry types, while the NSC types form $N_n^{(nsc)}/2$ pair symmetry types; hence, the number of pair types is

$$P_n = N_n^{(sc)} + \tfrac{1}{2} N_n^{(nsc)}, \qquad (3)$$

while the number of (ordinary) symmetry types is

$$N_n = N_n^{(sc)} + N_n^{(nsc)}. \qquad (4)$$

Applying formula (2) to this situation, one finds that

$$P_n = \frac{1}{n!2^n} \sum_{t \in G} J(t), \qquad (5)$$

where $J(t)$ is the number of pairs $(f, \bar{f})$ left invariant by operation t of the group G. Now, a pair $(f, \bar{f})$ is left invariant by t if, and only if, either

1) $t(f)=f$, or
2) $t(f)=\bar{f}$.

Let $J_1(t)$ and $J_2(t)$ be the numbers of pairs corresponding to cases 1) and 2), respectively. Thus, $J(t)=J_1(t)+J_2(t)$.

Suppose that the operation t permutes the 2^n vertices of the n cube into $K(C)$ cycles, where C is the operation class to which t belongs. There are $2^{K(C)}$ ways in which these vertices can be labelled with 0's and 1's so that the labelling is constant over each cycle. Each such labeling defines a Boolean function invariant under operation t. Hence, $J_1(t)=2^{K(C)-1}$, since there are half as many pairs as there are functions.

* Received by the PGEC, February 23, 1960; revised manuscript received, May 9, 1960.

[1] "Synthesis of Electronic Computing and Control Circuits," The Staff of the Computation Laboratory, Harvard University, Harvard University Press, Cambridge, Mass.; 1951.

[2] R. A. Higgonet and R. A. Grea, "Logical Design of Electrical Circuits," McGraw-Hill Book Co., Inc., New York, N. Y.; 1958. See "Table of Four-Relay Circuits," by E. F. Moore, pp. 195–216.

[3] D. Slepian, "On the number of symmetry types of Boolean functions of n variables," *Can. J. Math.*, vol. 5, no. 2, pp. 185–193; 1953. Also Bell Telephone System Monograph 2154.

[4] W. H. Kautz, "State-logic relations in autonomous sequential networks," *Proc. EJCC*, Boston, Mass.; December, 1958.

[5] M. Karnaugh, "The map method for synthesis of combinational logic circuits," *Trans. AIEE (Commun. and Electronics)*, vol. 72, pp. 593–599; November, 1953.

[6] G. Pólya, "Sur les types des propositions composées," *J. Symbolic Logic*, vol. 5, pp. 98–103; 1940.

[7] S. W. Golomb, "On the classification of Boolean functions," IRE TRANS. ON INFORMATION THEORY, vol. IT-5, p. 185; May, 1959.

[8] All operations conjugate to a given operation are of the form ata^{-1} where a is an arbitrary operation of G.

On the other hand, $J_2(t)$ counts the number of pairs $(f, \bar{f})$ such that $t(f)=\bar{f}$. Any such function f corresponds to a labeling of the vertices of the n cube with 0's and 1's alternating as one proceeds around any cycle. Clearly, this is possible only if each cycle is of even length. In that case, there are two possible labelings for each cycle, and the labelings are independent from cycle to cycle. Hence, for all cycles even, there are $2^{K(C)}$ distinct labelings meeting the requirement $t(f)=\bar{f}$; if some cycles are of odd length, there are no such labelings.

Let the operation classes C be separated into two categories—those classes C' whose operations permute the vertices of the n cube into some odd cycles, and those classes C'' whose operations result in all even cycles. We then have

$$J(t) = 2^{K(C')-1}, \quad \text{for } t \text{ in class } C', \text{ and}$$
$$J(t) = 2^{K(C'')}, \quad \text{for } t \text{ in class } C''. \tag{6}$$

By combining (5) and (6), we obtain

$$P_n = N_n^{(sc)} + \frac{1}{2} N_n^{(nsc)}$$
$$= \frac{1}{n!2^n}\Big[\sum_{C'} 2^{K(C')-1} n_{C'} + \sum_{C''} 2^{K(C'')} n_{C''} \Big].$$

But, by virtue of (4), we also have

$$N_n = N_n^{(sc)} + N_n^{(nsc)}$$
$$= \frac{1}{n!2^n}\Big[\sum_{C'} 2^{K(C')} n_{C'} + \sum_{C''} 2^{K(C'')} n_{C''} \Big].$$

It follows that

$$N_n^{(nsc)} = \frac{1}{n!2^n} \sum_{C'} 2^{K(C')} n_{C'} \tag{7}$$

and

$$N_n^{(sc)} = \frac{1}{n!2^n} \sum_{C''} 2^{K(C'')} n_{C''}. \tag{8}$$

Thus, the number of self-complementary (hence neutral) symmetry types is given by Slepian's sum (1) restricted to the operation classes C'', while the number of non-self-complementary symmetry types (neutral or not) is given by the sum (1) extended over the remaining operation classes C'. In Table I are shown some values of N_n, $N_n^{(sc)}$, and $N_n^{(\text{neutral})}$ computed with the aid of (7) and (8), and Slepian's formula[3] for the number $N_n^{(\text{neutral})}$ of neutral symmetry types in n variables.

TABLE I

NUMBERS OF SELF-COMPLEMENTARY SYMMETRY TYPES, NEUTRAL SYMMETRY TYPES, AND ALL SYMMETRY TYPES FOR $n=1, 2, 3, 4$ AND 5

n	$N_n^{(sc)}$	$N_n^{(\text{neutral})}$	N_n
1	1	1	3
2	2	2	6
3	6	6	22
4	42	74	402
5	4094	169,112	1,228,158

One notes from Table I that the ratio of $N_n^{(sc)}$ to $N_n^{(\text{neutral})}$ appears to approach zero as n increases. This is strikingly opposite to what one might expect on the basis of the cases $n=1$, 2 and 3 alone, where all the neutral symmetry types are also self-complementary. Thus, for large n it appears that *most* of the neutral types are non-self-complementary, and that self-complementary types are, in the long run, a rather rare phenomenon. Even for $n=5$, the self-complementary types constitute only about 2.4 per cent of all neutral symmetry types. On the other hand, SC neutral symmetry types certainly exist for all values of n. (The even and odd parity functions have this property, for example.)

It is perhaps pertinent to inquire as to the physical significance of the distinction made above between operations of the group G which belong to classes of category C' and those belonging to category C''. We first point out that any group operation t may be represented in terms of an autonomous sequential network[4] consisting of shift registers and inverters. These components are connected in closed loops, the loops being unconnected to each other, as in Fig. 3, for example. In any loop containing an even number of inverters, these inverters may be removed; and in any loop with an odd number of inverters, all but a single inverter may be removed. The first kind of loop corresponds to what Slepian[3] calls an *e-cycle.* The second kind corresponds to Slepian's *o-cycle.* In replacing an even (or odd) number of inverters by zero (or one) inverter, we change the *specific* operation of the group but not its *class*, C. Thus these networks provide canonical representations of the equivalence classes of the hypercube group. The state diagram of the network then represents the permutation induced by the group operation on the vertices of the n cube.

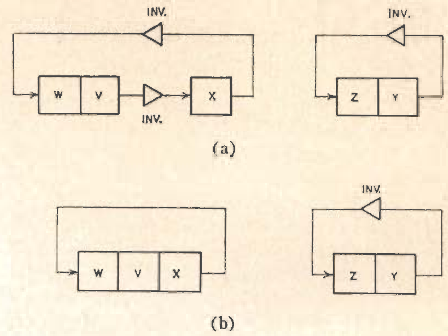

Fig. 3—(a) Network representation of the variable transformation: $v\to w$, $w\to\bar{x}$, $x\to\bar{v}$, $y\to z$, $z\to\bar{y}$. (b) Canonical network representation equivalent to (a).

Now the operation classes of category C'' (all permutation cycles of vertices of even length) may be shown to correspond to operations with some *o*-cycles. Likewise, the classes C' may be seen to consist solely of operations made up of *e*-cycles. (These results are implicit in Slepian's work,[3] although no explicit mention is made there of the fact.) In terms of our network model of the situation, the classes C' consist of those operations represented canonically by inverter-free networks, while the classes C'' consist precisely of those operations whose canonical representations contain one or more inverters.

Since the inverter-free nets are particularly simple to analyze, it is most convenient to calculate $N_n^{(nsc)}$ rather than $N_n^{(sc)}$. The determination of the cycle set $[k_1, \cdots, k_{K(C)}]$ for a given network of category C' may be carried out by means of Slepian's Table I, or more directly, by means of the results given by Elspas[9] relating to the cycle set of a circulating shift register. The whole cycle set for all 2^n vertices (*i.e.*, states) is then obtained by the process of cycle set multiplication.[10]

An interesting and as yet unsolved problem is that of obtaining asymptotic expressions of the numbers of SC and NSC neutral symmetry types for large n.

BERNARD ELSPAS
Stanford Res. Inst.
Menlo Park, Calif.

[9] B. Elspas, "The theory of autonomous linear sequential networks," IRE TRANS. ON CIRCUIT THEORY, vol. CT-6, pp. 45–60; March, 1959. See especially p. 60.

[10] *Ibid.*, p. 50.

Reprinted from IRE TRANSACTIONS ON *ELECTRONIC COMPUTERS*
Volume EC-9, Number 2, June, 1960

PRINTED IN THE U.S.A.