ON THE NUMBER OF SYMMETRY TYPES OF BOOLEAN FUNCTIONS OF n VARIABLES

DAVID SLEPIAN

1. Introduction. In recent years Boolean Algebra has come to play a prominent role in the analysis and synthesis of switching circuits [**1**; **4**]. One general synthesis problem in which this algebra has proved useful is the following. Let there be given n input leads each of which can assume one of two possible states. It is desired to construct a network with these n input leads and a single output lead also capable of assuming either of two states. Furthermore, the state of the output lead for each of the 2^n states of the input leads is prescribed. Techniques are now available for solving this problem and under various assumptions as to the meaning of "best," techniques for finding the "best" network are also available [**1**].

The operation performed by the above network can be described by a Boolean function of n variables. Thus if the variables $x_1, x_2, \ldots, x_n$ represent the states of the n input leads (each x takes values 0 or 1), then the state of the output lead can be given by a Boolean function $f(x_1, x_2, \ldots, x_n)$. Specifying the function f determines the synthesis problem and under suitable restrictions leads to the synthesis of a definite physical network to realise f. From a physical point of view, however, it is immaterial how the n input leads are labelled or which of the two states any lead can assume is called zero or one. Therefore any Boolean function that can be obtained from f by permuting and (or) complementing one or more variables must be regarded as corresponding to the same physical network as f. It is convenient to define two Boolean functions of n variables to be of the same type if one of the functions can be obtained from the other by the process of permuting and (or) complementing one or more variables. There are then only as many distinct physical switching networks of the sort described above as there are types of Boolean functions of n variables. It is the purpose of this paper to enumerate the types of Boolean functions.

The argument to be used in determining N_n, the number of types of Boolean functions of n variables, is as follows. In §2 it is noted that there are only $\mu = 2^{2^n}$ possible Boolean functions of n variables and that each of these μ functions can be written as a linear combination of a certain set of 2^n simple Boolean functions, s_v. The operations of permuting and (or) complementing one or more of the n variables of a Boolean function constitute a finite group, O_n, simply isomorphic with the hyper-octahedral group. Under the operations of O_n, the s_v are permuted among themselves, as are also the μ Boolean functions of n variables. The permutations of the latter furnish a representation, D, of

Received November 20, 1951.

https://doi.org/10.4153/CJM-1953-020-x Published online by Cambridge University Press

O_n, which is shown to be reducible containing the identity representation N_n times. The theory of group characters then yields

$$N_n = \frac{1}{2^n n!} \sum n_C \chi_C$$

where n_C is the number of elements of class C of O_n, χ_C in the character of class C in the representation D, and the summation is over all classes of O_n. Similar considerations give rise to a formula for $N_n^{(m)}$, the number of types of Boolean functions that are a linear sum of exactly m of the functions s_v. To make computations from the formulae of §2, it is necessary to know n_C, χ_C and quantities $\lambda_i^{(C)}$ which serve to define the cycle structure of the permutation of the s_v induced by any element of class C of O_n. In §3 these quantities are determined. A resumé of the computational procedure is given in §4 and results of computations performed are presented.

2. Formulae for N_n and $N_n^{(m)}$. It is well known that any Boolean function of n variables can be uniquely expanded in the form

$$f_u(x_1, x_2, \ldots, x_n) = \sum_{v=0}^{2^n-1} \epsilon_{uv}\, s_v \tag{1}$$

where the ϵ_{uv} can take values zero or one and the s_v are the 2^n simple Boolean functions

$$s_0 = x_1 x_2 \ldots x_n, \quad s_1 = x_1 x_2 \ldots x_n', \quad \ldots, \quad s_{2^n-1} = x_1' x_2' \ldots x_n',$$

i.e., the functions obtained by priming the product $x_1 x_2 \ldots x_n$ in all possible 2^n ways. (The prime is used to denote complementation.) Since each ϵ can assume one of two values, there are only $\mu = 2^{2^n}$ possible Boolean functions of n variables so that $u = 0, 1, \ldots, \mu - 1$.

Agreeing to arrange the x's of any s_v so that their subscripts are in natural order, we can represent any s by an n-position symbol consisting of zeros or ones, the ith position of the symbol being zero if x_i is not primed and one otherwise. We agree to label the s's so that the symbol for s_v is the integer v expressed in binary notation. Similarly each f_u can be specified by the 2^n zeros or ones, ϵ_{uv}, and we order the f's so that u is the number whose binary expression is $\epsilon_{u0}\, \epsilon_{u1} \ldots \epsilon_{u[2^n-1]}$.

It is readily seen that the operations of permuting and (or) complementing the variables of a Boolean function form a finite group, O_n, the multiplication law being defined by successive application of the operators to f. We adopt the customary cycle notation for permutations so that, for example, $\sigma = (123)(45)$ applied to f means replace x_1 by x_2, replace x_2 by x_3, etc. Complementation may be expressed by an operator N_i where i is written in binary notation. Thus N_{10011} applied to f means prime x_1, x_4, and x_5, and $N_i\sigma$ means first apply σ to f, then apply N_i.

We now define the complementation operator $N_{\sigma i}$ to mean the operator N_j where j is the binary expression obtained by applying the permutation σ to

https://doi.org/10.4153/CJM-1953-020-x Published online by Cambridge University Press

the places of the binary symbol i. For example,

$$N_{(125)(64)101100} = N_{001011},$$

the symbol in the first place being replaced by the symbol in the second place, etc. With this convention, the law $N_i\sigma = \sigma N_{\sigma i}$, $\sigma N_i = N_{\rho i}\sigma$, $\rho = \sigma^{-1}$ is readily established so that every element of O_n can be written in the form $N_i\sigma$. Since there are 2^n complementation operators N_i, and $n!$ permutation operators, σ, the order of O_n is $2^n n!$. The group is recognized as being simply isomorphic to the hyper-octahedral group [**5**; **6**], the group of symmetries of the hyper-octahedron in n-dimensional Euclidean space. This group is also the group of symmetries of the hyper-cube in n-space, and the permutations of the s_v effected by the elements of O_n correspond to the permutations of the vertices of the hyper-cube under the various symmetry operations.

The totality of operations, H, of O_n which leave any particular f_u invariant form a subgroup of O_n of order h, say. H will possess $r = 2^n n!/h$ left cosets under O_n. It is easily shown then that operating on f_u by all the elements of O_n will result in exactly r distinct Boolean functions. These r functions are of one type and are all the functions of this type. The permutations of these r functions under the operations of O_n when written as permutation matrices furnish a representation of O_n of dimension r. This representation is just the permutation representation furnished by the left cosets of H and is therefore reducible containing the identity representation exactly once [**2**, p. 94].

Now the μ Boolean functions (1) are also permuted among themselves under the operations of O_n and these permutations when written as permutation matrices furnish a representation, D, of dimension μ of O_n. From the remarks of the preceding paragraph, it follows that D is reducible since it contains each of the r-dimensional representations once. D therefore contains the identity representation exactly N_n times, where N_n is the number of types of Boolean functions of n variables, and we can write

$$N_n = \frac{1}{2^n n!}\sum n_C\, \chi_C\,. \tag{2}$$

Here n_C is the number of elements of class C of O_n, χ_C is the character of class C in the representation D, and the summation is over all classes of O_n.

Under the operations of O_n, the quantities s_v are clearly permuted among themselves. It is easily shown, however, that two elements of the same class of O_n give rise to permutations of the s_v that have the same cycle structure. We are thus led to investigate the number of f_u left invariant when the s_v are permuted according to some fixed cycle structure, for this number is the character of the representation D of the class of O_n which permutes the s_v according to this fixed cycle structure.

Let σ be a permutation of the s_v into K cycles of length λ_i $(i = 1, 2, \ldots, K)$. We have

$$\sum_1^K \lambda_i = 2^n.$$

https://doi.org/10.4153/CJM-1953-020-x Published online by Cambridge University Press

Consider now the matrix ϵ_{uv} of equation (1). The μ rows of this array are the binary representations of the integers from 0 to $\mu - 1$, and these rows may be labelled by the f_u. Similarly the columns may be labelled by the s_v. On permuting the columns of the ϵ matrix according to σ, the rows considered as numbers expressed in binary form are no longer in natural order and their new order specifies the permutation of the f's induced by σ. Clearly only those f's will be left invariant which have either all zeros or all ones in the λ_i particular columns effected by the ith cycle of σ ($i = 1, 2, \ldots, K$). Of the μ rows of ϵ, a fraction $2/2^{\lambda_i}$ have this property, so that there are

$$\mu \prod_{i=1}^{K} 2/2^{\lambda_i} = 2^K$$

f's left invariant under σ. We can therefore rewrite (2) in the form

$$N_n = \frac{1}{2^n n!} \sum 2^{K(C)} n_C \tag{3}$$

where $K(C)$ is the number of cycles in which the s_v are permuted by any element of class C of O_n.

In a similar manner we can obtain a formula for the number of types of Boolean functions, $N_n^{(m)}$, that have exactly m non-zero terms in their expansion (1). Under the operations of O_n, these f's are permuted among themselves and these permutations written as matrices furnish a reducible representation of O_n. If the character of this representation is $\chi_C^{(m)}$, we have

$$N_n^{(m)} = \frac{1}{2^n n!} \sum n_C \, \chi_C^{(m)} . \tag{4}$$

To determine $\chi_C^{(m)}$ consider the rows of the matrix ϵ_{uv} of (1) corresponding to those

$$\binom{2^n}{m}$$

f's containing exactly m s's. Let σ be the permutation of the s_v induced by an element of class C of O_n and let σ consist of cycles of length

$$\lambda_i^{(C)} \left(i = 1, 2, \ldots, K; \ \sum_1^{K(C)} \lambda_i^{(C)} = 2^n \right).$$

$\chi_C^{(m)}$ is the number of these rows left invariant on permuting the columns according to σ and is therefore the number of ways in which m can be obtained as a sum of terms taken from the series $\lambda_1, \lambda_2, \ldots, \lambda_K$, no term occurring more than once in any one sum. Thus $\chi_C^{(m)}$ is the coefficient of y^m in

$$\prod_{i=1}^{K(C)} (1 + y^a)$$

where $a = \lambda_i^{(C)}$. Equation (4) now becomes

$$N_n^{(m)} = \text{coefficient of } y^m \text{ in } \ \frac{1}{2^n n!} \sum n_C \prod_{i=1}^{K(C)} (1 + y^a) \tag{5}$$

https://doi.org/10.4153/CJM-1953-020-x Published online by Cambridge University Press

where the sum is over all classes of O_n and the elements of class C effect a permutation of the s's with cycle structure $\lambda_i^{(C)}$.

Formula (5) has been given by Pólya [**3**] who has computed values of $N_n^{(m)}$ for $n = 1, 2, 3, 4$. Pólya, however, gives no means of determining the quantities n_C and $a = \lambda_i^{(C)}$. It is believed that formula (3) for N_n is new.

Equation (3) is a special case of the solution to the following more general enumeration problem. Each vertex of the hyper-cube in Euclidean n-space can be marked with one of p colors. Two such paintings of the hyper-cube are said to be of the same type if one can be obtained from the other by a symmetry operation of the hyper-cube. The number of types of paintings is

$$\frac{1}{2^n n!}\sum p^{K(C)} n_C.$$

3. Classes of O_n and the quantities n_C and $\lambda_i^{(C)}$. Details of the classes of O_n have been worked out by Young [**6**]. It will therefore suffice here to set down briefly a notation for the classes and a system for determining the class of a given element, $N_i\sigma$, of O_n.

Let $(ab\ldots)$ be a typical cycle of σ where $a, b, \ldots$ are certain of the symbols $1, 2, \ldots, n$. The complementation operator N_i will indicate that either an even or an odd number of the variables $x_a, x_b, \ldots$ are to be primed by the operation $N_i\sigma$. In the former case we refer to $(ab\ldots)$ as an e-cycle of the element $N_i\sigma$, in the latter case an o-cycle. With this terminology, the elements of O_n can be classified by the following scheme. Let σ consist of α_i cycles of length i so that

$$\sum_1^n i\alpha_i = n.$$

Let β_i be the number of the α_i cycles of length i that are e-cycles of $N_i\sigma$, so that the possible values of β_i are $\beta_i = 0, 1, 2, \ldots, \alpha_i$ $(i = 1, 2, \ldots, n)$. To every element of O_n there then corresponds a symbol

$$(\alpha_1, \alpha_2, \ldots \alpha_n;\ \beta_1, \beta_2, \ldots, \beta_n)$$

or $(\alpha; \beta)$ for short.

It is shown in [**6**] that two elements of O_n are in the same class if and only if they have the same $(\alpha; \beta)$ symbol. A simple calculation shows that the number of elements in the class $(\alpha; \beta)$ of O_n is

$$n_{(\alpha;\,\beta)} = n!\prod_{i=1}^n \frac{2^{(i-1)\alpha_i}}{\beta_i!\,(\alpha_i - \beta_i)!\,i^{\alpha_i}} \tag{6}$$

and the number of classes in O_n is

$$\sum \prod_{i=1}^n (\alpha_i + 1)$$

where the sum is over all partitions of n.

We now inquire as to the cycle structure of the permutation of the s_v induced by an operation N_σ of the class C of O_n. Since all elements of the class C permute the s_v in the same cycle structure, it will suffice to consider the effect of a particularly simple element of this class. We choose the element $N_i\sigma$ where the complementation operator N_i does not prime any of the variables permuted by the e-cycles of $N\sigma$ and where N_i primes only one variable from each set of variables permuted by the various separate o-cycles of $N\sigma$. The permutation of the s_v induced by $N_i\sigma$ can best be studied by representing the s_v by the numbers from 0 to $2^n - 1$ written in binary scale and listed in natural order in a column. The effect of $N_i\sigma$ on the s_v is given by first permuting the columns of this array according to σ, and then in one column corresponding to each o-cycle interchanging the role of zero and one. The new array is again a list of the numbers from 0 to $2^n - 1$ in binary scale, and the new order of these numbers specifies the permutation of the s_v effected by $N_i\sigma$. Suppose the cycles of σ are of length

$$\lambda_i \left(i = 1, 2, \ldots, K; \sum_1^K \lambda_i = n\right).$$

In the original array in any given row and in the λ_i columns corresponding to the ith cycle of σ, there will appear zeros and ones specifying in binary form a number, ξ_i, between 0 and $2^{\lambda_i} - 1$. We can accordingly specify the 2^n s_v by K-place symbols

$$(\xi_1, \xi_2, \ldots, \xi_K), \qquad \xi_i = 0, 1, \ldots, 2^{\lambda_i} - 1.$$

The ith cycle of σ, whether an e-cycle or an o-cycle of $N_i\sigma$, has the effect of permuting the 2^{λ_i} values of ξ_i. Let us suppose the cycle structure of this permutation is

$$\alpha_j^{(\lambda_i)} \quad (j = 1, 2, \ldots, 2^{\lambda_i}),$$

i.e., there are

$$\alpha_j^{(\lambda_i)}$$

cycles of length j in the permutation of the 2^{λ_i} values of ξ_i, induced by the operation of the ith cycle of σ. (This number depends on whether the cycle is an e- or an o-cycle of $N_i\sigma$.) It is clear that a knowledge of the α's suffices to define the cycle structure of the permutation of the s_v as a function of $N_i\sigma$.

For example, if $K = 2$ and the permutation of the values of ξ_1 has a cycle of length a and the permutation of the values of ξ_2 has a cycle of length b, then the s_v will have ab/c cycles of length c, where c is the least common multiple of a and b. This may be seen as follows. Without loss of generality we may assume the cycle of length a to be $(12\ldots a)$ and the cycle of length b to be $(12\ldots b)$ and $a < b$. We wish to determine the cycle structure of the permutation of the ab symbols (ξ_1, ξ_2) where $\xi_1 = 1, 2, \ldots, a$; $\xi_2 = 1, 2, \ldots, b$. Now $(1, 1)$ will be replaced by $(2, 2)$, $(2, 2)$ by $(3, 3), \ldots, (a, a)$ by $(1, a + 1)$, etc. We return to $(1, 1)$ after c steps. Similarly, starting with any of the ab symbols (ξ_1, ξ_2) the original symbol is again obtained after c steps. Since there are only ab symbols, they must be permuted in ab/c cycles each of length c.

These observations for $K = 2$ can be extended to arbitrary K. The following simple calculus for determining the cycle structure of the permutations of the s_v is then obtained. For each $i = 1, 2, \ldots, K$ form the expression

$$P(\lambda_i) = \sum_{j=1}^{2^{\lambda_i}} \alpha_j^{(\lambda_i)} z_j$$

in the indeterminates z_j. Define multiplication of the z's by

(7) $$z_a z_b = (ab/c)\, z_c$$

where c is the least common multiple of a and b (an associative law of multiplication when extended to three or more factors). The product

$$\bar{P} = \prod_1^K P(\lambda_i)$$

can then be expanded in the form $\Sigma\, \alpha_i z_i$. The α_i are positive integers giving the number of cycles of length i in the permutation of the s_v induced by $N\sigma$.

There remains only the problem of obtaining the quantities

$$\alpha_j^{(\lambda_i)}.$$

These quantities depend not only on the length λ_i of the cycle in question, but on whether the cycle is an e- or o-cycle. For an e-cycle, $\alpha_j^{(\lambda)}$ can be obtained as follows. Let the numbers from 0 to $2^\lambda - 1$ be written in binary form in natural order in a column. The effect of an e-cycle of length λ on this array may be obtained by removing the left-hand column of the array and writing it in again as the right-hand column. Each original binary number is then doubled modulo $2^\lambda - 1$, and the permutation is easily written; e.g., for $\lambda = 3$ we have (0) (1, 2, 4) (3, 6, 5) (7) and $\alpha_1^{(3)} = 2, \alpha_3^{(3)} = 2$ and all other $\alpha^{(3)}$ are zero. The o-cycle case can be obtained from the e-cycle case by interchanging the zeros and ones in the column of the array in which these symbols alternate from row to row. This corresponds to left-multiplying the permutation obtained in the e-cycle case by the permutation

$$(0, 1)\ (2, 3) \ldots (2^n - 2, 2^n - 1).$$

For $\lambda = 3$, we find $(0, 1, 3, 7, 6, 4)(2, 5)$ whence $\alpha_2^{(3)} = 1$, $\alpha_6^{(3)} = 1$ and all other $\alpha^{(3)}$ are zero. Table I lists the $P(\lambda)$ for e- and o-cycles of length $\lambda = 1, 2, 3, 4, 5, 6$.

TABLE I

λ	$P(\lambda_e)$	$P(\lambda_o)$
1	$2\, z_1$	z_2
2	$2\, z_1 + z_2$	z_4
3	$2\, z_1 + 2\, z_3$	$z_2 + z_6$
4	$2\, z_1 + z_2 + 3\, z_4$	$2\, z_8$
5	$2\, z_1 + 6\, z_5$	$z_2 + 3\, z_{10}$
6	$2\, z_1 + z_2 + 2\, z_3 + 9\, z_6$	$z_4 + 5\, z_{12}$

It can be shown that the rows of Table I can be extended successively to larger values of λ as follows. For $\lambda = n$ and the case of an e-cycle, the only z's occurring in $P(\lambda_e)$ (e denotes that the cycle of length λ is an e-cycle) are those whose subscripts are integral divisors of n, and every such z occurs. Every such z except z_n has occurred previously in the $P(\lambda_e)$ table and the coefficients of these z's in $P(n_e)$ are taken to be identical with the coefficients in previous occurrences of these z's. Thus

$$P(n_e) = \sum_1^{n-1} \alpha_i z_i + x z_n$$

where only x is unknown; x is then given by

$$x = \left(2^n - \sum_1^{n-1} i \alpha_i\right) \Big/ n.$$

$P(n_o)$ is obtained in a somewhat similar manner. The only z's occurring in $P(n_o)$ are those whose subscripts are integral divisors of $2n$ but are not integral divisors of n, and every such z occurs. All such z's except z_{2n} have occurred previously in the $P(\lambda_o)$ table and the coefficients of these z's in $P(n_o)$ are taken to be identical with the coefficients of these z's in previous occurrences. $P(n_o)$ is thus

$$\sum_1^{2n-1} \alpha_i z_i + x z_n$$

where only x is unknown; x is given by

$$x = \left(2^n - \sum_1^{2n-1} i \alpha_i\right) \Big/ 2n.$$

4. Computational scheme and results of computations. The procedure developed above may be summarized as follows. A partition of n into positive integers,

$$n = \sum_1^K \lambda_i ,$$

is written by listing the λ_i in any order. The subscript e or o is added to each λ_i. Each of the distinct possible symbols obtained in this manner specifies a class of O_n and all classes of O_n are obtained. The cycle structure of the permutation of the s_v induced by all elements of any class C is obtained by forming

$$\bar{P} = \prod_1^K P(\lambda_i) = \sum \alpha_i z_i$$

(using (7)) where the appropriate $P(\lambda)$ are taken from Table I; α_i is the number of cycles of length i in the permutation of the s_v induced by an element of class C whence the quantities $\lambda_i^{(C)}$ of (5) are obtained. $K(C)$ of (3) is given by $\sum \alpha_i$ and n_C by (6) so that N_n and $N_n^{(m)}$ can then be obtained from (3) and (5).

This computational scheme was used to obtain the following values of N_n:

n	1	2	3	4	5	6
N_n	3	6	22	402	1,228,158	400,507,806,843,728

References

1. Harvard Computation Laboratory Staff, *Synthesis of electronic computing and control circuits* (Cambridge, Mass., 1951).
2. F. D. Murnaghan, *The theory of group representations* (Baltimore, 1938).
3. G. Pólya, *Sur les types des propositions composées*, J. Symbolic Logic, *5* (1940), 98-103.
4. C. E. Shannon, *The synthesis of two-terminal switching circuits*, Bell System Tech. J., *28* (1949), 59-98.
5. J. A. Todd, *The groups of symmetries of the regular polytopes*, Proc. Cambridge Phil. Soc., *27* (1931) 212-231.
6. A. Young, *On quantitative substitutional analysis*, Proc. London Math. Soc. (2), *31* (1930), 273-288.

Bell Telephone Laboratories, Inc.
Murray Hill, New Jersey