T H E U N I V E R S I T Y O F M I C H I G A N

COLLEGE OF ENGINEERING
Department of Electrical Engineering
Information Systems Laboratory

Technical Note

# SYMMETRIC AND PARTIALLY SYMMETRIC BOOLEAN FUNCTIONS

Michael A. Harrison

ORA Project 04879

under contract with:

UNITED STATES AIR FORCE
AERONAUTICAL SYSTEMS DIVISION
CONTRACT NO. AF 33(657)-7811
WRIGHT-PATTERSON AIR FORCE BASE, OHIO

administered through:

OFFICE OF RESEARCH ADMINISTRATION ANN ARBOR

February 1962

TABLE OF CONTENTS

SUMMARY

Algorithms for detecting symmetric and partially symmetric Boolean functions are derived using the generators of the symmetric group. Certain properties of symmetric functions are discussed, in particular the behavior of symmetric functions under the group of permutations and complementations. These results indicate the connection between ordinary symmetric functions and symmetric functions of mixed variables.

# I. INTRODUCTION

Since almost all switching functions are arbitrarily complex, it is desirable to restrict our attention to special classes of functions in practical design problems. Two classes of interesting functions are the symmetric and partially symmetric functions. If we consider the realization of switching functions by relay contacts, and if the number of variables n is reasonably large, then an arbitrary switching function asymptotically requires $\frac{2^n}{n}$ contacts, while a symmetric function requires at most $n^2$ contacts, and a partially symmetric function of n variables, symmetric in k of them, requires at most min $\Big((k + 1)(\lambda(n - k) + k), (k + 1)(2^{n-k} + k - 2) + 2\Big)$. Thus we easily see that these classes of functions are more economical to realize than an arbitrarily selected function.*

The only algorithms for detecting whether a function is symmetric are due to Caldwell[2] and McCluskey[8]. Caldwell's method uses a generalization of the Karnaugh map to detect symmetric functions. Since the use of this map becomes prohibitive for even a moderate number of variables, we shall exclude this technique from our consideration. The algorithm to be presented here competes favorably with the method of McCluskey, but its real importance is that it can

*The question of complexity of switching functions was raised by Shannon.[11] He was able to show that for any $\epsilon > 0$ and $n > n_0(\epsilon)$ that $(1 - \epsilon)\frac{2^n}{n} < \lambda(n) < (1 + \epsilon)\frac{2^{n+2}}{n}$, and he conjectured that for any $\epsilon > 0$, almost all functions have a complexity exceeding $1 - \epsilon$. In a sequence of papers, Povarov and Lupanov improved these results, and Lupanov finished the problem by showing that $\lambda(n) \sim \frac{2^n}{n}$. These authors have extended their results and obtained some information about propositional functions. It is gratifying to see an application of switching theory to logic.

be generalized to an algorithm for detecting partially symmetric functions.

The method to be given here applies only to functions of unmixed variables, i.e., functions of $x_1,\ldots,x_n$ or functions of $\bar{x}_1,\ldots,\bar{x}_n$, but not functions of, say, $x_1, \bar{x}_2,\ldots,x_n$.

Example. $S_{\{2,3\}}(x_1,x_2,x_3) = x_1x_2 + x_2x_3 + x_1x_3$ is a symmetric function, while $S_{\{2,3\}}(x_1,\bar{x}_2,x_3) = x_1x_2 + \bar{x}_2x_3 + x_1x_3$ is a mixed symmetric function and is excluded in our considerations.

The larger problem of functions of mixed variables is intimately connected with the group invariance of switching functions and will be considered in a later paper. In Section VII of this report the connection between symmetric functions of mixed and unmixed variables will be discussed.

## II. PERMUTATION GROUPS

To derive the algorithm to be given, a few results from the elementary theory of permutation groups are required. A reader familiar with the symmetric group may profitably skip this section.

Consider the set $S = \{1,2,\ldots,n\}$. By a permutation of the set S we mean a one-to-one mapping from S onto S. The set of all permutations of $S = \{1,2,\ldots,n\}$ forms a group called the symmetric group of n letters, denoted by $\mathcal{P}_n$. The group operation is the composition of the mappings. We shall establish the convention of applying the mappings from the right. That is, if $\alpha,\beta \in \mathcal{P}_n$, then $(\alpha\beta)(x) = \alpha(\beta(x))$. The order of $\mathcal{P}_n$ is clearly n! The usual notation for permutations will be employed. Consider the permutation $\alpha$ in $\mathcal{P}_6$ which replaces 1 by 3, replaces 3 by 5, replaces 5 by 1, interchanges 2 and 4, and leaves 6 in-

variant. We write

$$\alpha = (135)(24)(6)$$

There is no reason to write the cycles of length one, so they will be omitted henceforth.

Example. Let $\alpha = (135)(24)$ and $\beta = (23)$.

Then $\alpha\beta = (25134)$ and $\beta\alpha = (12435)$.

We now derive a few elementary facts about $\mathcal{P}_n$.

Theorem 2.1. Any permutation $\sigma \in \mathcal{P}_n$ can be written as a product of disjoint cycles.

Proof. Choose any $\sigma \in \mathcal{P}_n$ and select a number $a_1 \in \{1,\ldots,n\}$. Construct $\sigma a_1 = a_2$, $\sigma a_2 = a_3, \ldots$ until we reach a number already in the list, say $\sigma a_k = a_i$ $(1 \leq i \leq k)$. The predecessor of $a_j$ is $a_{j-1}$ for $j > 1$, and therefore $\sigma a_k = a_1$. Thus we have $\sigma = (a_1,\ldots,a_k)$. If $k < n$, the remaining numbers are permuted among themselves by $\sigma$. The argument is repeated on the remaining numbers. Since n is finite, the argument will terminate with $\sigma = (a_1,\ldots,a_k)(b_1,\ldots,b_m)\ldots(c_1,\ldots,c_p)$.

Corollary 2.2. Any $\sigma \in \mathcal{P}_n$ may be written as a product of transpositions. A transposition is a cycle of length two, i.e. $(ab)$.

Proof. Note that $(a_1,\ldots,a_k) = (a_1a_2)(a_1a_3)\ldots(a_1a_k)$.

The following lemma is very useful in actually carrying out computations with permutations. Two elements of a group, say $\sigma$ and $\tau$, are said to be conjugate it there exists an element $\rho$ in the group such that $\sigma = \rho\tau\rho^{-1}$. The next lemma says that if one has $\tau$ and $\rho$ in our cyclic notation, $\rho\tau\rho^{-1}$ may be calculated by performing the permutation $\rho$ on the digits in the cycles of $\tau$.

Lemma 2.3. If $\tau = (a_{11},\ldots,a_{1p})(a_{21},\ldots,a_{2q})\ldots(a_{k1},\ldots,a_{kr})$ and $\rho$ replaces

$a_{ij}$ by $b_{ij}$, then $\rho\tau\rho^{-1} = (b_{11},\ldots,b_{1p})(b_{21},\ldots,b_{2q})\ldots(b_{k1},\ldots,b_{kr})$.

Proof.

$$\rho^{-1} : b_{ij} \longrightarrow a_{ij}$$

$$\tau : a_{ij} \longrightarrow a_{i,j+1}$$

$$\rho : a_{i,j+1} \longrightarrow b_{i,j+1}$$

Thus $b_{ij} \longrightarrow b_{i,j+1}$ by $\rho\tau\rho^{-1}$ as claimed.

Example. Suppose $\tau = (12)(345)$ and $\rho = (1345)$. Then

$$\rho\tau\rho^{-1} = (23)(145).$$

Corollary 2.4. Two permutations are conjugate in $\mathcal{P}_n$ if and only if they have the same number of cycles of each length.

Proof. The preceding lemma shows that conjugate permutations have the same cycle structure. Conversely, suppose $\sigma = (a_{11},\ldots,a_{1p})(a_{21},\ldots,a_{2q})\ldots(a_{k1},\ldots,a_{kr})$ and $\tau = (b_{11},\ldots,b_{1p})\ldots(b_{k1},\ldots,b_{kr})$. Then take $\rho$ as the permutation which replaces $a_{ij}$ by $b_{ij}$, and then $\tau = \rho\tau\rho^{-1}$.

## III. SYMMETRIC FUNCTIONS

For any switching function of n variables $f(x_1,\ldots,x_n)$ and any permutation $\sigma\in\mathcal{P}_n$, we define their product $\sigma f$ as follows:

$$\sigma f(x_1,\ldots,x_n) = f(x_{\sigma(1)},\ldots,x_{\sigma(n)}).$$

Example. Suppose $\sigma = (124)$ and $f(x_1,x_2,x_3,x_4) = \bar{x}_1(x_3 + x_4) + \bar{x}_2x_3$,

then $\sigma f(x_1,x_2,x_3,x_4) = f(x_2,x_4,x_3,x_1) = \bar{x}_2(x_1 + x_3) + x_3\bar{x}_4$.

Definition 3.1. A switching function f is said to be symmetric if and only

if $\sigma f = f$ for every $\sigma \in \mathcal{P}_n$.*

To detect whether a function is symmetric, the use of the above definition would require n! tests, but it will be shown that the symmetric group on n letters is generated by only two permutations, one of which is a transposition. Since $\mathcal{P}_n$ is not cyclic for $n \geq 3$, there is no algorithm with fewer than two tests.

Lemma 3.2. $\mathcal{P}_n$ is generated by the n - 1 transpositions (1 n), (2 n), (3 n)..., (n - 1,n).

Proof. Every element $\sigma \in \mathcal{P}_n$ may be written as a product of transpositions by by corollary 2.2. It is sufficient to show that all $\frac{n(n-1)}{2}$ transpositions can be obtained from these n - 1 transpositions. This is trivial because

$$(i\ j) = (i\ n)(j\ n)(i\ n).$$

Theorem 3.3. $\mathcal{P}_n$ is generated by the two permutations $\alpha = (1\ 2\ 3\ \ldots\ n-1)$ and $\beta = (n-1,n)$.

Proof. It will be shown that one can obtain the permutations which occur in the hypothesis of the previous lemma with these two permutations. Corollary 2.4 tells us how to proceed. We compute the conjugates of $\beta$ by $\alpha^i$ for i = 1, ...,n - 1. Using lemma 2.3, we get

---

*The definition of a symmetric function which has been given is not quite correct. Let $\mathcal{O}$ be a commutative ring with identity, and $\mathcal{O}[x_1,\ldots x_n]$ be the ring of polynomials in the indeterminants $x_1,\ldots,x_n$ over $\mathcal{O}$. The mapping $\phi_\sigma : \sigma \to \sigma f$ is an automorphism of $\mathcal{O}$ and the mapping $\sigma \to \phi_\sigma$ is an isomorphism of $\mathcal{P}_n$ onto the automorphism group of $\mathcal{O}$.

The symmetric functions form a ring $\mathcal{E}$ and in fact $\mathcal{O}[x_1,\ldots x_n]$ is a Galois extension of $\mathcal{E}$ of degree n! and whose Galois group is isomorphic to $\mathcal{P}_n$. Our definition identifies $\mathcal{P}_n$ and the automorphism group, but since these groups are isomorphic this is a harmless identification.

$$\alpha\beta\alpha^{-1} = (1\ n)$$

$$\alpha^{i}\beta\alpha^{-1} = (i\ n) \text{ for } i = 2,\ldots,n-2$$

$$\alpha^{n-1} = 1 \text{ implies } \alpha^{n-1}\beta\alpha^{-(n-1)} = (n-1,n)$$

By lemma 3.2, $\alpha$ and $\beta$ generate $\mathcal{P}_n$.

Theorem 3.4. *If any group $\mathcal{G}$ is generated by $\alpha_1,\ldots,\alpha_r$, and if $\alpha_i f = f$ for $i = 1,\ldots,r$ then $\sigma f = f$ for any $\sigma \in \mathcal{G}$.*

*Proof.* The argument is a trivial induction on the number of generators r.

The algorithm is now apparent. If a function is invariant under (1 2 ...n - 1) and (n - 1,n), then the function is symmetric. Restating this in functional notation we get the following corollary.

Corollary 3.5. *A Boolean function $f(x_1,\ldots,x_n)$ is symmetric if and only if $f(x_1,x_2,\ldots,x_{n-1},x_n) = f(x_2,x_3,\ldots,x_{n-1},x_1,x_n)$ and $f(x_1,\ldots,x_{n-2},x_{n-1},x_n) = f(x_1,\ldots,x_{n-2},x_n,x_{n-1})$.*

## IV. EXAMPLES AND COMPUTATIONAL SUGGESTIONS

The algorithm is extremely easy to use. If the function is in expanded normal form and if the fundamental products are represented as n-tuples of zeros and ones in the usual way, then one may form a matrix which represents the function. This matrix will have n columns and as many rows as there are terms in the normal form expansion. To check for invariance under (n - 1,n) merely interchange the last two columns of the matrix. This may permute the rows of the matrix, but if a reordering of rows is performed which returns the new matrix to the original matrix, then the function is invariant under (n - 1,n).

To check for invariance under (1 2 ...n - 1), move all the columns to the left one position except the nth column which remains unmoved. The n - 1 column is replaced by the first column. We now reorder and check. These calculations may be carried out with permutation matrices, but there appears to be no reason to do so.

Example. Let $f = \bar{x}_1x_2x_3x_4 + x_1\bar{x}_2x_3x_4 + x_1x_2\bar{x}_3x_4 + x_1x_2x_3\bar{x}_4$. We will use a double arrow ($\longleftrightarrow$) to indicate the correspondence between a function and its matrix; we will use ($\sim$) to denote an equivalence relation between matrices such that if A and B are two matrices of the same order comprised of zeros and ones, then $A \sim B$ iff A may be obtained from B by permuting the rows of B.

$$f \longleftrightarrow \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$(34)f \longleftrightarrow \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \longleftrightarrow f$$

Thus this function is invariant under (3 4).

$$(1\ 2\ 3)f \longleftrightarrow \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \longleftrightarrow f$$

This function is symmetric. The row weights are the "a-numbers." (Recall that the a-numbers are integers between zero and n such that when any "a" of the variables are one, then the function is one.)

Example. Let $g = x_1\bar{x}_2\bar{x}_3\bar{x}_4 + x_1\bar{x}_2\bar{x}_3x_4 + x_1\bar{x}_2x_3\bar{x}_4$.

$$g \longleftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$(1\ 2\ 3)g \longleftrightarrow \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \longleftrightarrow g$$

This function is therefore not symmetric.

David E. Wood has programmed this algorithm for the IBM-7090. Wood's program determines if a function has partial symmetries, and if so, the program determines in which variables the function is symmetric. If the function is totally symmetric, then the program determines the "a" numbers of the function.

## V. PARTIALLY SYMMETRIC FUNCTIONS

The importance of the algorithm given in the previous section is that it can be generalized to the case of partially symmetric functions.

Definition 5.1. A Boolean function of n variables $f(x_1,\ldots,x_n)$ is said to be partially symmetric if and only if there exists a permutation $\sigma \in \mathcal{P}_n$ different from the identity permutation such that $\sigma f = f$.

The set of permutations $\sigma$ such that $\sigma f = f$ forms a subgroup of $\mathcal{P}_n$ since if $\sigma f = f$ and $\tau f = f$, then $(\sigma\tau)(f) = \sigma(\tau(f)) = \sigma(f) = f$.* The detection of symmetric functions was accomplished by finding a set of convenient generators for $\mathcal{P}_n$. The detection of partially symmetric functions involves finding a set of generators for the set of all subgroups of $\mathcal{P}_n$.

*A subgroup $\mathcal{H}$ is a subset of the domain of the group $\mathcal{G}$ closed under the group operation, containing inverses and the identity. The requirement about containing the identity may be dropped since if the first two conditions are satisfied then $a \in \mathcal{H}$ implies $a^{-1} \in \mathcal{H}$ which implies $aa^{-1} = 1 \in \mathcal{H}$. In a finite group, the requirement of containing inverses is redundant. Cf. Ref. 5, Section 1-2, problem 4.

The algorithm is provided by corollary 2.2. One computes $\sigma f$ for every transposition $\sigma$. There are $\frac{n(n-1)}{2}$ transpositions. The set of all transpositions which leave f invariant will immediately tell us which variables the function is partially symmetric in. The calculations must be performed on the expanded normal form. The algorithm is illustrated in the following example.

Example. Let $f = x_1x_2x_3x_4 + x_1\bar{x}_2\bar{x}_3x_4 + x_1\bar{x}_2x_3x_4 + \bar{x}_1x_2\bar{x}_3x_4 + \bar{x}_1x_2x_3x_4 + \bar{x}_1\bar{x}_2\bar{x}_3x_4$. The transpositions which must be used in the test are (1 2), (1 3), (1 4), (2 3), (2 4), and (3 4). It is important to use the permutations in this order. If the function is invariant under all of (1 2),...,(1 4), then the function is totally symmetric because (i j) = (1 i)(1 j)(1 i). These transpositions are another set of generators of $\mathcal{P}_n$.*

$$f \longleftrightarrow \begin{pmatrix} 0&0&0&1\\ 0&1&0&1\\ 0&1&1&1\\ 1&0&0&1\\ 1&0&1&1\\ 1&1&1&1 \end{pmatrix}$$

$$(1\ 2)f \longleftrightarrow \begin{pmatrix} 0&0&0&1\\ 1&0&0&1\\ 1&0&1&1\\ 0&1&0&1\\ 0&1&1&1\\ 1&1&1&1 \end{pmatrix} \sim \begin{pmatrix} 0&0&0&1\\ 0&1&0&1\\ 0&1&1&1\\ 1&0&0&1\\ 1&0&1&1\\ 1&1&1&1 \end{pmatrix} \longleftrightarrow f$$

In a similar fashion we see that all the other transpositions do not leave f invariant. Thus f is partially symmetric in $x_1$ and $x_2$.

*Finding a set of generators and relations for $\mathcal{P}_n$ has been a popular indoor sport since 1897 when Burnside and Moore each gave generators and relations for $\mathcal{P}_n$. Cf. Ref. 4. $\mathcal{P}_n$ has a geometric interpretation as the symmetry group of the n - 1 dimensional simplex.

## VI. THE GEOMETRIC REPRESENTATIONS OF SYMMETRIC FUNCTIONS

In this section some geometrical interpretations of symmetric functions are discussed. Theorem 6.2 is well known; theorems 6.4 and 6.5 are due to Lee, but are reworded here to obtain greater clarity. Theorem 6.6 is due to Lupanov.

The reader is assumed to be familiar with the usual representation of switching functions on the n-dimensional cube as developed by Lee.[7]

Definition 6.1. The n + 1 elementary symmetric functions are defined as follows:

$$\sigma_0(x_1,\ldots,x_n) = \bar{x}_1\bar{x}_2\ldots\bar{x}_n$$

$$\sigma_1(x_1,\ldots,x_n) = x_1\bar{x}_2\ldots\bar{x}_n + \bar{x}_1x_2\ldots\bar{x}_n + \ldots + \bar{x}_1\bar{x}_2\ldots x_n$$

$$\vdots$$

$$\sigma_n(x_1,\ldots,x_n) = x_1x_2\ldots x_n$$

$\sigma_i(x_1,\ldots,x_n)$ has $\binom{n}{i}$ terms in its normal form expansion and $\sigma_i(x_1,\ldots,x_n) = 1$ if and only if any i of its variables are ones. Therefore, $\sigma_i(x_1,\ldots,x_n) = S_{\{i\}}(x_1,\ldots,x_n)$ for $i = 0,\ldots,n$. Of course $i \neq j$ implies $\sigma_i(x_1,\ldots,x_n)\sigma_j(s_1,\ldots,x_n) = 0$ and $\sum_{j=0}^{n} \sigma_j(x_1,\ldots,x_n) = 1$.

Theorem 6.2. Every symmetric function has a unique expansion as a sum of elementary symmetric functions. This theorem is the analog of the symmetric function theorem for ordinary polynomials. It has been discovered (and re-discovered) by Lee,[7] Povarov,[9] myself,[5] and probably others.

Let X and Y be two vertices of the n-cube. We write $X = (x_1,\ldots,x_n)$ and $Y = (y_1,\ldots,y_n)$ where $x_i, y_i \in \{0,1\}$ (cf. Fig. 1 for an example in three dimensions). We define the distance between X and Y to be $d(X,Y) = \sum_{i=1}^{n} (x_i \oplus y_i)$ where the

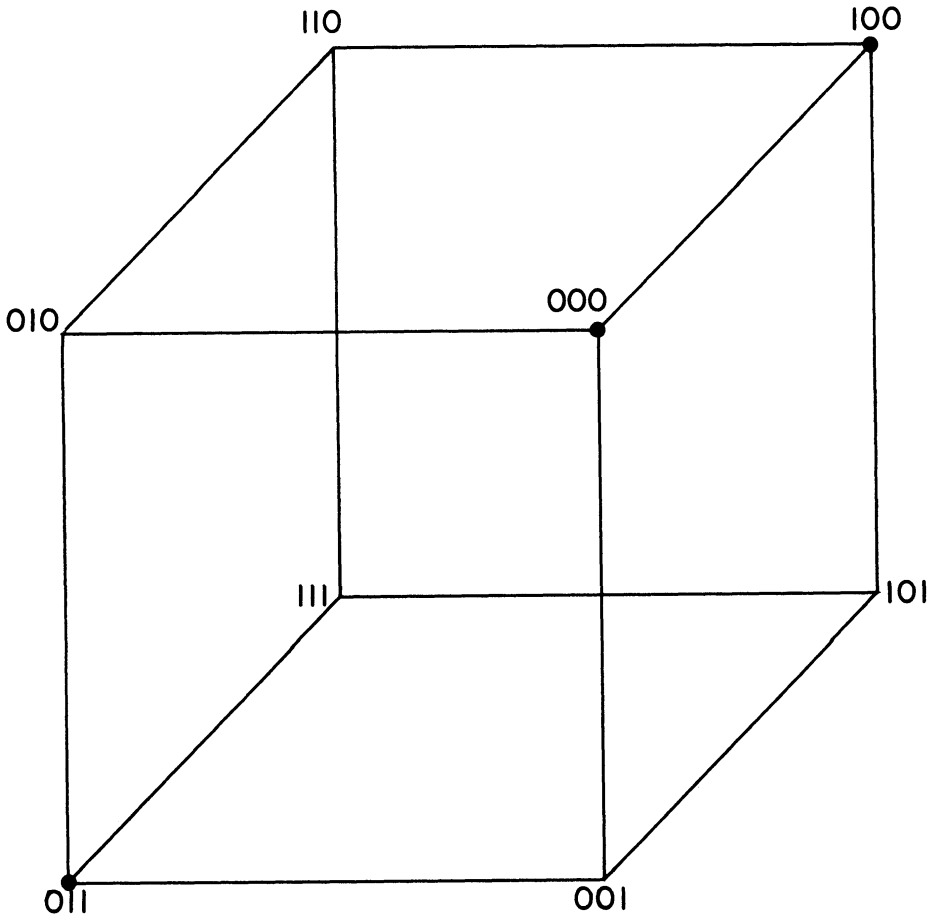


Fig. 1. The graphical representation of the function $f(x_1,x_2,x_3) = \bar{x}_2\bar{x}_3 + \bar{x}_1x_2x_3$.

summation indicates addition of natural numbers. d(X,Y) satisfies the axioms of a metric.[5]

Definition 6.3. We denote a sphere of radius r about the center C as $\mathcal{K}_r^C$ ($\mathcal{K}$ stands for Kugel) where

$$\mathcal{K}_r^C = \{X \mid d(X,C) = r\}.$$

These spheres have two centers, one at radius r and one at radius n - r assuming $r \leq n - r$. The centers are bit-wise complements of one another. A sphere of radius r has $\binom{n}{r}$ points.

Theorem 6.4. The elementary symmetric switching functions $\sigma_i(x_1 \ldots x_n)$ (i =

0,...n) form spheres on the n-cube. The elementary symmetric functions have centers at (0,...,0) and (1,...,1) with radii i and n - i, respectively. Conversely, any such sphere corresponds to an elementary symmetric function.

Proof: Merely note that $\sigma_i(x_1,\ldots,x_n)$ has $\binom{n}{i}$ terms in its expanded normal form. Each term is of weight i, so its radius from the origin is i. The converse is obvious.

Arbitrary spheres on the n-cube correspond to elementary symmetric functions of mixed variables.

Theorem 6.5. A sphere of radius r on the n-cube with center C corresponds to an elementary symmetric function of mixed variables and conversely. The positions in which C has a one are the variables which are complemented. The radius of the sphere is the subscript of the elementary symmetric function.

Proof: The complementation operator which takes C into (0,...,0) [and the far center into (1,...,1)] preserves the radius. Use theorem 6.4.

Example. The set of points

| | |
|---|---|
| (0,0,0,1) | (1,0,1,1) |
| (0,0,1,0) | (1,1,0,1) |
| (0,1,0,0) | (1,1,1,0) |

forms a sphere with radius 2 and centers (1,0,0,0) and (0,1,1,1). Complementing $x_1$, we get

| | |
|---|---|
| (1,0,0,1) | (0,0,1,1) |
| (1,0,1,0) | (0,1,0,1) |
| (1,1,0,0) | (0,1,1,0) |

This function is $\sigma_2(\bar{x}_1,x_2,x_3,x_4)$.

Caldwell's graphical technique[2] is in fact an attempt at finding these spheres.

The geometry of the elementary symmetric functions of n variables is rather interesting. The points of the spheres may be connected to form regular n - 1 dimensional polytopes for all the elementary symmetric functions of 2, 3 and 4 variables. The function $\sigma_2(x_1,x_2,x_3,x_4,x_5)$, however, furnishes a counter example to the general conjecture. This function has $\binom{5}{2} = 10$ vertices. There is no regular four-dimensional polytope with 10 vertices.[3] See Fig. 2 for an example. These spheres may be classified in other ways also.

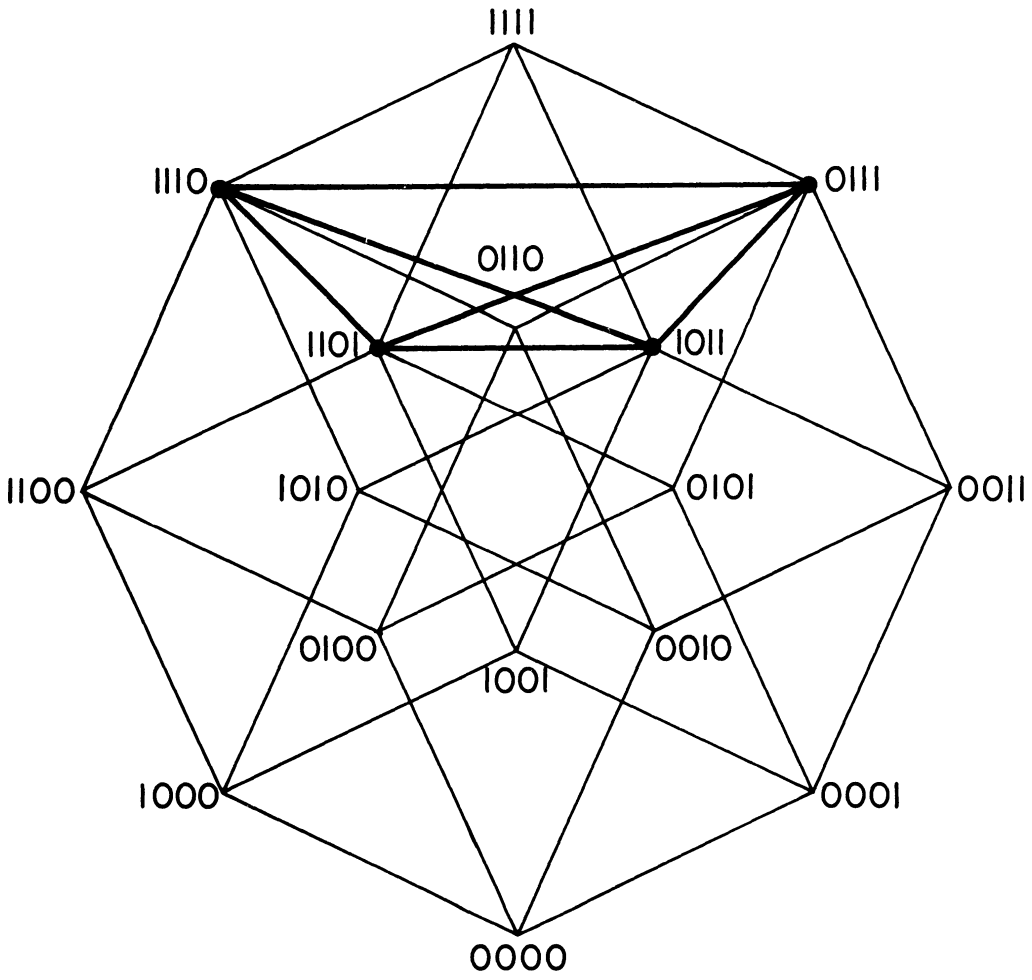


Fig. 2. The symmetric function $\sigma_3(x_1,x_2,x_3,x_4)$. The heavy lines form a regular tetrahedron whose edges are two units long as measured with the discrete metric.

These spheres may be exploited in many ways. The following algebraic identity enables one to construct complete decoding networks which asymptotically require one-half the contacts in a tree network.[5]

Theorem 6.6. *If $\sigma_1(z_1,\ldots,z_n)$ is the characteristic function of the sphere of radius one with center $C = (c_1,\ldots,c_n)$, then*

$$z_i^{\bar{c}_i}\,\sigma_1(z_1,\ldots,z_n) = z_1^{c_1}\cdots z_{i-1}^{c_{i-1}}\, z_i^{\bar{c}_i}\, z_{i+1}^{c_{i+1}}\cdots z_n^{c_n}$$

where

$$\bar{c}_i = \begin{cases} 1 & \text{if } c_i = 0 \\ 0 & \text{if } c_i = 1 \end{cases}$$

for $i = 1,\ldots,n$.

When one investigates the symmetric functions algebraically, one immediately looks for elementary symmetric functions. The $\delta$-functions about to be introduced have the same form as the elementary symmetric functions in an ordinary commutative ring. They are, however, not as convenient to work with, and they are of secondary importance. The reader will recognize the $\delta$-functions as the majority functions so widely used in work on reliability.

Definition 6.7. *The $\delta$-functions are defined as follows:*

$$\delta_0 = 1$$

$$\delta_1 = \sum_{i=1}^{n} x_1$$

$$\delta_2 = \sum_{1\leq i<j\leq n} x_i x_j$$

$$\vdots$$

$$\delta_n = x_1 x_2 \cdots x_n$$

Thus $\delta_k(x_1,\ldots x_n) = 1$ iff at least k of the variables are 1. The following theorem gives some simple identities about the $\delta$ functions.

Theorem 6.8.

a. $\delta_k(x_1,\ldots x_n) = \sum_{0\le i_1<i_2<\ldots<i_k\le n} x_{i_1}\ldots x_{i_k} = S_{\{k,k+1,\ldots,n\}}(x_1,\ldots,x_n) = \overline{S}_{\{0,1,\ldots,k-1\}}(x_1,\ldots,x_n)$ for $k = 1,\ldots,n$

b. $\delta_j \circ \delta_k = \delta_{\max(j,k)}$.

c. $\delta_i + \delta_j = \delta_{\min(i,j)}$.

d. $\delta_k(x_1,\ldots x_n) = \overline{S}_{\{k,\ldots,n\}}(x_1,\ldots x_n) = S_{\{0,1,\ldots k-1\}}(x_1,\ldots x_n)$

e. $\delta_j \le \delta_k$ iff $j \ge k$ where $\le$ is the usual partial ordering relation of a Boolean algebra.[5]

These functions are sufficient to serve as "generators" of the symmetric functions.

Theorem 6.9. Every symmetric function has a unique expansion in terms of $\delta_i$ and $\overline{\delta}_i$.

Proof: Note that $\sigma_k(x_1,\ldots,x_n) = \delta_k(x_1,\ldots,x_n)\overline{\delta}_{k+1}(x_1,\ldots,x_n)$. Apply theorem 6.2.

## VII. MISCELLANEOUS PROPERTIES OF SYMMETRIC FUNCTIONS

We list some elementary properties of symmetric functions due to various writers, and exploit some of the results to discuss the relation of symmetric functions to mixed symmetric functions.

Theorem 7.1 (Lee).

a. If f is a symmetric function of n variables, then

$$f(x_1,\ldots,x_n) = \sum_{i\in I} \sigma_i(x_1,\ldots,x_n) = \sum_{i\in I} S_{\{i\}}(x_1,\ldots,x_n)$$

where $I$ is some subset of $\{0,1,\ldots,n\} = Z_{n+1}$.

b. If $f$ is symmetric, then $\bar{f}$ is symmetric and

$$\bar{f}(x_1,\ldots x_n) = \sum_{i\in(Z_{n+1}-I)} \sigma_i(x_1,\ldots x_n) = \sum_{i\in(Z_{n+1}-I)} S_{\{i\}}(x_1,\ldots x_n).$$

c. $x_1 \oplus \ldots \oplus x_n = \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \sigma_{2k+1}(x_1,\ldots x_n)$ where $\left[\frac{n-1}{2}\right]$ denotes the largest integer not exceeding $\frac{n-1}{2}$.

d. Defining $x_j^{e_j} = \begin{cases} x_j & \text{if } e_j = 1 \\ \overline{x_j} & \text{if } e_j = 0, \end{cases}$ we have

$$x_1^{e_1} \oplus \ldots \oplus x_n^{e_n} = \begin{cases} x_1 \oplus \ldots \oplus x_n & \text{if } \sum_{i=1}^{n} e_i \equiv 1 \bmod 2 \\ \overline{x_1 \oplus \ldots \oplus x_n} & \text{if } \sum_{i=1}^{n} e_i \equiv 0 \bmod 2 \end{cases}$$

Caldwell's paper[6] produced some interesting discussions. The following theorem due to Karnaugh is contained in this discussion.[6]

Theorem 7.2 (Karnaugh).

$$\sigma_a(x_1,\ldots,x_n) = \sum_{\substack{i+j=a \\ 0\le i\le k \\ 0\le j\le n-k}} \sigma_i(x_1,\ldots x_k)\, \sigma_j(x_{(k+1)},\ldots,x_n)$$

One can interpret geometrically the set of points in the summation. Draw the i, j plane and consider points with integer coordinates such that $i\in[0,k]$ $j\in[0,n-k]$. Then the set of points over which we sum is the straight line of slope -1 passing through (a,0) and (0,a). This theorem allows us to decompose

the set of variables into disjoint subsets. This theorem may be proven by induction on k. For k = 1, this is Caldwell's expansion theorem for symmetric functions.

Karnaugh's theorem generalizes immediately to the following result which was implicitly stated in Ref. 6.

Theorem 7.3. A function $f(x_1,\ldots,x_n)$ is symmetric if and only if

$$f(x_1,\ldots x_n) = \sum_{r=0}^{m} \sum_{\substack{i+j=a \\ 0\le i\le k \\ 0\le j\le n-k}} \sigma_i(x_1,\ldots x_k)\sigma_j(x_{k+1},\ldots x_n)$$

for any $0 \le k \le n$.

Proof: Note that $S_{\{a_1,\ldots,a_m\}}(x_1,\ldots,x_n) = \sum_{r=0}^{m} \sigma_{a_r}(x_1,\ldots x_n)$

and apply theorem 7.2.

The rather unpleasant indices in the above summation can be simplified. The following form of theorem 7.3 is due to Povarov.

Theorem 7.4. A Boolean function $f(x_1,\ldots,x_n)$ is symmetric if and only if

$$f(x_1,\ldots,x_n) = \sum_{i=0}^{k} \sigma_i(x_1,\ldots,x_k)S_{\{a_{i1}a_{i2}\ldots a_{im_i}\}}(x_{k+1},\ldots,x_n)$$

where $0 \le k \le n$ and each diagonal directed downwards from left to right in a point lattice of $n - k + 1$ horizontal coordinates and $k + 1$ vertical points is either completely occupied or unoccupied by the points $(i,a_{ij})$.

The procedure given in this theorem allows us to easily characterize the numbers given in the summation of theorem 7.3.

Example. We will illustrate the procedure for $f(x_1,\ldots x_{10}) = S_{\{0,1,2,5,7\}}$

$(x_1,x_2,\ldots,x_{10})$. Taking k = 6 and drawing Fig. 3

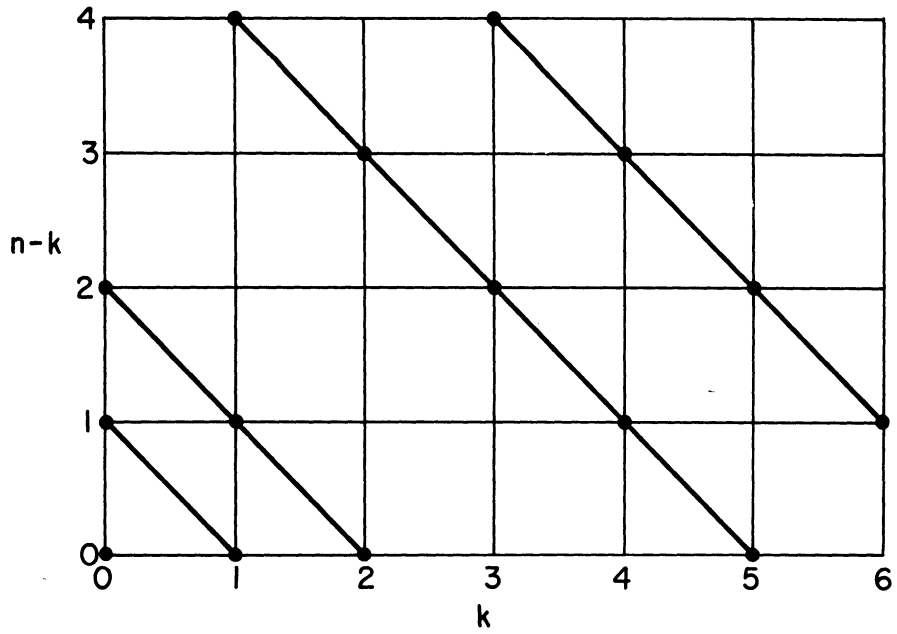


Fig. 3. The set of operating points for the symmetric function $S_{\{0,1,2,5,7\}}(x_1,\ldots,x_{10})$.

$$
\begin{aligned}
f(x_1,\ldots x_{10}) \;=\; & S_0(x_1,\ldots x_6)\cdot S_{\{0,1,2\}}(x_1,\ldots,x_{10}) \\
& + S_1(x_1,\ldots x_6)\, S_{\{0,1,4\}}(x_7,\ldots x_{10}) + \\
& S_2(x_1,\ldots x_6)\, S_{\{2,3\}}(x_7,\ldots x_{10}) + \\
& S_3(x_1,\ldots x_6)\, S_{\{2,4\}}(x_7,\ldots x_{10}) + \\
& S_4(x_1,\ldots x_6)\, S_{\{1,3\}}(x_7,\ldots x_{10}) + \\
& S_5(x_1,\ldots x_6)\, S_{\{0,2\}}(x_7,\ldots x_{10}) + \\
& S_6(x_1,\ldots x_n)\, S_{\{1\}}(x_7,\ldots x_{10})
\end{aligned}
$$

The calculation involved taking each "a" number of f and decomposing it into the sum of two numbers i and j such that

$$
\begin{aligned}
& i + j = a \\
& 0 \leq i \leq 6 \\
& 0 \leq j \leq 4
\end{aligned}
$$

The calculations are:

1. a = 0 (0,0)
2. a = 1 (0,1) and (1,0)
3. a = 2 (0,2), (1,1), (2,0)
4. a = 5 (1,4), (2,3), (3,2), (4,1), (5,0)
5. a = 7 (3,4), (4,3), (5,2), (6,1)

These points completely occupy the diagonals in Fig. 3. The numbers $(i,a_{ij})$ are called the operating points of the function. The $a_{ij}$ are graphically found as the ordinates along the vertical line x = i which intersects the diagonals.

The importance of this theorem is that it is useful in the group invariance problem for determining the structure of the equivalence classes containing symmetric functions. The reader is assumed to be familiar with group invariance of switching functions as introduced by Shannon. Let $\mathcal{J}_n$ be the group of complementations and permutations.* Two functions are said to be equivalent iff they are in the same transitivity set, i.e., iff there exists an element of $\mathcal{J}$ which maps one function into the other. Shannon described the structure of this group as the direct product of $C_2^n$ with $\mathcal{P}_n$ where $C_2^n$ denotes the direct product of the cyclic group of order two with itself n times. This is not correct. The situation is slightly more complicated. Actually, $\mathcal{J}_n = C_2 \wr \mathcal{P}_n$

*The group $\mathcal{J}_n$ of complementations and permutations was famous prior to its connection with logic and switching theory. $\mathcal{J}_n$ is the symmetry group of the n-cube or measure polytope which has Schläfli symbol $\{4,3^{n-2}\}$. It is also the symmetry group of the reciprocal polytope having Schläfli symbol $\{3^{n-2}, 4\}$. This is called the cross polytope, and it is the n-dimensional analog of the octahedron. The group may also be described as the symmetry group of the n-dimensional Cartesian frame formed by n mutually perpendicular lines through a point. There is also a connection between this group $\mathcal{J}_n$ and the automorphism group of the free group with n generators.

where $C_2 \wr S_n$ denotes the Wreath product of $C_2$ and $S_n$. The structure of this group will be discussed in a forthcoming report.

Theorem 7.5 (Povarov). The number of equivalence classes under $S_n$ which contain at least one symmetric function is

$$2^n + 2^{\left[\frac{n}{2}\right]} + 2\left[\frac{1}{2}(n+1)\right] - n - 1$$

where $[x]$ is the largest integer not exceeding $x$.

Theorem 7.6 (Povarov). The number of functions equivalent to some symmetric function under $S_n$ is

$$2^{2n} - 2^{n+1} + 4$$

These two theorems tell us the connection between ordinary symmetric functions and symmetric functions of mixed variables. Theorem 7.5 counts the number of different networks necessary to realize symmetric functions. Theorem 7.6 gives the total number of symmetric functions of mixed and unmixed variables. Caldwell distinguished between these two types of functions in his paper. The discussion by Washburn[12] appears to have convinced Caldwell that no distinction is necessary. Caldwell should have stuck to his original position because the functions are different while the physical networks are essentially the same. The confusion stems from misinterpretation of the meaning of group invariance. To sum up, equivalent functions under $S_n$ have essentially the same network associated with them.

Example. The two elementary symmetric functions $\sigma_i(x_1,\ldots,x_n)$ and $\sigma_{n-i}(x_1,\ldots,x_n)$ are equivalent under $S_n$. They have essentially the network realization, but are quite different.

The following theorem shows that any function of n variables is a symmetric

function of a sufficiently large number of variables.

Theorem 7.7. Any function $f(x_1,\ldots x_n)$ of n variables may be written as a symmetric function of $2^n - 1$ variables. If decimal numbers are used to denote the terms of the disjunction normal form of f, then these are the "a" numbers of the symmetric function of $2^n - 1$ variables.

Proof: Consider the mapping which sends $f(x_1,\ldots,x_n) \longrightarrow S_{\{a_1,\ldots a_k\}}$ $(x_1,x_2,x_2,\ldots,x_n\ldots x_n)$ where each $x_i$ is replaced by $2^{i-1}$ $x_i$'s in the image and each $a_i$ corresponds to a term in the expanded normal form of f. Thus the image is a function of $\sum_{i=1}^{n} 2^{i-1} = 2^n - 1$ variable. This mapping sends every function of n variables into a symmetric function of $2^n - 1$ variables. The mapping is clearly onto, one-to-one, and preserves +, $\cdot$ and - $\cdot$ The mapping is really an isomorphism of the Boolean algebra of all $2^{2^n}$ functions of n variables onto the Boolean algebra of symmetric functions of $2^n - 1$ variables.

This theorem does not have an immediate practical application. Most functions of n variables require $2^n/_n$ contacts for large n. A function realized by this scheme requires $(2^n - 1)^2$ contacts. This latter number is larger than $2^n/_n$ for $n \geq 2$. Thus it is more expensive to realize an arbitrary function as a symmetric function of a larger number of variables.

## VIII. SOME ALGEBRAIC RESULTS

The symmetric functions of n variables form a Boolean algebra of $2^{n+1}$ elements. The elementary symmetric functions are the atoms. This remark indicates why the $\delta$-functions were not called the elementary symmetric functions of the Boolean algebra. This Boolean algebra is a quotient algebra of the

Boolean algebra of all switching functions module a certain ideal. The choice of this ideal is not unique, but the resulting quotient algebras are isomorphic. Each residue class contains $2^{2^n} - (n+1)$ functions.

The partially symmetric functions of the same k ($2 \leq k \leq n - 1$) variables form a Boolean algebra containing the Boolean algebra of symmetric functions. This algebra has $2^{(k+1)2^{n-k}}$ elements.

All the results may be simplified using the theory of ideals (or filters) in a Boolean algebra. Associated with these decompositions are synthesis procedures. For instance, any function f may be realized as a function of a symmetric function and a function in the ideal which determines the algebra of symmetric functions. This ideal is the kernel of the homomorphism. It has also been shown directly that almost all functions are not partially symmetric.

REFERENCES


1. N. Bourbaki, Éléments De Mathématique, I, Les Structures Fondamentales De L'Analyse, Libre II, Algebre, Hermann, Paris; 1959, Chapitres 1 et 4.

2. S. H. Caldwell, "The Recognition and Identification of Symmetric Switching Functions," A.I.E.E. Transactions, Part I, Communications and Electronics, Volume 73, pp. 142-146; May 1954.

3. H. S. M. Coxeter, Regular Polytopes, Metheusen and Co. Ltd., London; 1948.

4. H. S. M. Coxeter and W. O. J. Moser, Generators and Relations for Discrete Groups, Springer-Verlag, Berlin; 1957.

5. M. A. Harrison, "Notes for a Course in Switching and Automata Theory," unpublished.

6. M. Karnaugh, "Discussion" (of [7]), A.I.E.E. Transactions, Part I; Communications and Electronics, Volume 73, pp. 146-147; May 1954.

7. C. Y. Lee, "Switching Functions on an n-Dimensional Cube," A.I.E.E. Transactions, Part I, Communications and Electronics, Volume 73, pp. 289-291; September 1954.

8. E. J. McCluskey, Jr., "Detection of Group Invariance or Total Symmetry of a Boolean Function," The Bell System Technical Journal, Volume 35, pp. 1445-1453; November 1956.

9. G. N. Povarov, "A Mathematical Theory for the Synthesis of Contact Networks with one Input and k Outputs," Proceedings of an International Symposium on the Theory of Switching, Part II, Harvard University Press, Cambridge, Massachusetts; 1959.

10. C. E. Shannon, "A Symbolic Analysis of Relay and Switching Circuits," A.I.E.E. Transactions, Volume 57, pp. 713-723; 1938.

11. C. E. Shannon, "The Synthesis of Two-Terminal Switching Circuits," The Bell System Technical Journal, Volume 28, pp. 59-98, January 1949.

12. S. H. Washburn, "Discussion" (of [7]), A.I.E.E. Transactions, Part I, Communications and Electronics, Volume 73, p. 146; May 1954.