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

Interim Engineering Report

COMBINATORIAL PROBLEMS IN BOOLEAN ALGEBRAS AND APPLICATIONS TO THE THEORY OF SWITCHING

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

June 1963

This report was also a dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in The University of Michigan, 1963.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF TABLES (CONT'D)

LIST OF TABLES (CONT'D)

LIST OF ILLUSTRATIONS

LIST OF APPENDICES

ABSTRACT

In recent years, the techniques of enumerative combinatorial analysis have been applied to Boolean algebras. It was Pólya who first showed that a natural group classifies Boolean functions into symmetry types. Thereafter, Shannon described how these symmetry types can be used in the theory of switching.

In this thesis, some new permutation groups on Boolean functions will be considered. The reasons for selecting these groups come from the motivations of switching theory. In each case, the cycle index, a multi-variate generating function for the cycle structure of the group is derived. An approach to combinatorial analysis which is capable of generalization is adopted in the presentation. In particular, it is the representation of a group as a permutation group (not as an abstract group) which determines the combinatorial properties of the group. The need for a structural theory of permutation groups is demonstrated and some results obtained. It is necessary for the purposes of combinatorial analysis to be able to decompose a group into suitable constituents and to construct the cycle index of the group in terms of the cycle indices of the component groups.

The cycle indices derived for the new groups provide new classification results for Boolean functions. The recent theorems of DeBruijn are applied to obtain refined results and to enumerate various new objects such as invertible Boolean functions, networks, and self-complementary classes of functions.

Finally, generalizations to Post algebras and other systems of interest are indicated in the paper.

CHAPTER I

INTRODUCTION AND HISTORY

1-1 Preliminaries

One of the basic characteristics of many areas of communication sciences is the finiteness of the objects under consideration. While finiteness of the object set sometimes results in easily derived decision procedures, many of the solutions to the problems of communication sciences arise as algorithms which are not "efficiently" computable. Even though the domain of the objects of interest may be finite, further structure and classification theorems need to be developed to facilitate computations in a practical sense. This thesis represents an approach to the solution of some of these problems. The motivation for studying these problems came from switching theory, and the presentation is made in a general way so that applications to other areas of interest may be made.

1-2 History

Felix Klein[20] characterized the fundamental problem of mathematics as that of finding the classification of systems under appropriate groups. This approach to group theory is now somewhat obscured by the abstract approach to mathematics, but the idea is that a group acting on a set of objects is, in some sense, a measure of the symmetry of the objects. The structure of the set may also be studied by examining the group. It is interesting to note that Klein's program has been carried out for certain kinds of geometries and also for logic[23]. A further account of Klein's program may be found in reference[42].

In 1937, Pólya published a paper in which a fundamental theorem on enumeration was proved[30]. If there is any single paper of outstanding importance in combinatorial analysis, it is Pólya's 100-page document. Some generalizations of Pólya's work were given in 1959 by DeBruijn[7]. The results of both authors, suitably modified for Boolean functions, will be used in this paper. In 1941, Pólya published a paper on the applications of his enumeration theorem to propositional functions[31]. While Pólya could not solve the general problem, he was able to count the number of symmetry types for $1 \leq n \leq 4$. In 1949, Shannon[37] indicated the practical importance of Pólya's ideas. Shannon showed that functions possessing non-trivial group invariance could be realized with fewer components than most functions. Later, the staff of the Harvard Computation Laboratory classified the 65,536 functions of four variables into the 402 symmetry classes and listed a representative from each class[17]. A variety of writers have compiled a table of minimal networks for the representatives of the classes. This table is extensively used in synthesis procedures[19].

In 1955, Slepian[40] constructed an ingenious calculus in order to solve the general problem posed by Pólya. Since that time, a number of papers have appeared containing reformulations of the problem (or the solution). In addition to this thesis, Robert Lechner[21], of Harvard University, is writing a thesis which is also concerned with many of the problems mentioned in the present work. Although Lechner and I have compared results, it should be explicitly stated that our methods and problems are different, and that both theses are independent works.

1-3 The Plan of the Thesis

In chapter two of this thesis, the mathematical background for the later sections is constructed. In addition to developing the fundamental enumeration theorems, several products of permutation groups are defined. The principal mathematical result of the thesis is given in chapter two, namely an algorithm for finding the cycle index of a new product of two permutation groups in terms of the cycle indices of the constituent groups.

Chapter three contains the construction of the cycle indices of the five most important groups in switching theory. In addition, the number of equivalence classes of Boolean functions is computed. Chapter four contains extensions of the ideas of chapter three. The idea of equivalence is refined and the results extended to networks and to invertible functions. Chapter five gives applications to problems of error correcting codes, graphs, sequential machines, and a generalization to Post algebras. Chapter six concludes with some unsolved problems.

II. MATHEMATICAL BACKGROUND

2-1. Introduction

In this section the fundamental theorems of enumerative combinatorial analysis will be derived. The discussion follows the papers of Golomb [13], Pólya [30], and DeBruijn [7]. Consider a finite set S consisting of s elements and a transformation group $\mathcal{J}$ acting on S. Consider two elements s_1 and s_2 to be equivalent under $\mathcal{J}$ if and only if there exists an $\alpha \in \mathcal{J}$ such that

$$s_1 = \alpha(s_2)$$

This relation will be denoted by $s_1 \sim s_2(\mathcal{J})$ which is read "s_1 is equivalent to s_2 under $\mathcal{J}$."

Lemma 1. $\sim(\mathcal{J})$ is an equivalence relation on S.

Proof. $s_1 = 1(s_1)$ where 1 is the identity map of $\mathcal{J}$ so that the relation is reflexive. If $s_1 \sim s_2(\mathcal{J})$, then $s_1 = \alpha(s_2)$ for some $\alpha \in \mathcal{J}$. Since $\mathcal{J}$ is a group, $s_2 = \alpha^{-1}(s_1)$ and the relation is symmetric. If $s_1 = \alpha(s_2)$ and $s_2 = \beta(s_3)$, then $s_1 = \alpha\beta(s_3)$ which shows that the relation is transitive and completes the proof.

The equivalence relation ~ decomposes the set S into equivalence classes, that is disjoint classes whose union is S. It is very natural to inquire into the number of classes. It is somewhat surprising that this question is so hard to answer in an efficient way. It is clear that in principle the problem is trivial since the group and the set are both finite. In fact, enumeration is not possible in many interesting cases (even with the use of high speed computers).

The first answer to this question came from a theorem due originally to Burnside (cf. [3], p. 191). Many people still use this approach because of its simplicity but it has computational shortcomings which will be pointed out. The result is obtained below.

Lemma 2. For any $s \in S$, $\mathcal{H}_s = \{\sigma \mid \sigma(s) = s\}$ is a subgroup.

Lemma 3. The number of elements in the equivalence class containing s is $[\mathcal{G} : \mathcal{H}_s]$, the index of $\mathcal{G}$ in $\mathcal{H}_s$.

Proof. By the above lemma, $\mathcal{H}_s$ is a subgroup of $\mathcal{G}$. Form $\mathcal{H}_s t$, the left coset of $\mathcal{H}_s$ containing t. We consider the mapping

$$\varphi_s : t \longrightarrow \mathcal{H}_s t \qquad t \in S$$

which maps elements of S into left cosets. Equivalent elements map into the same coset since

$$\varphi_s : t \longrightarrow \mathcal{H}_s t$$

$$\varphi_s : \alpha(t) \longrightarrow \mathcal{H}_s \alpha(t) = \{\sigma\alpha(t) \mid \sigma \in \mathcal{G}\} = \mathcal{H}_s t$$

As σ runs through $\mathcal{G}$, so does $\sigma\alpha$ (not necessarily in the same order) and we get the last equality above. Thus, φ_s maps equivalent elements onto cosets since given any coset $\mathcal{H}_s t$, t maps onto it. If we can show that φ is one-to-one, the result will be proven. Assuming that

$$\mathcal{H}_s t = \mathcal{H}_s u$$

is equivalent to $\qquad \sigma(t) = \rho(u)$

or $\quad t = \sigma^{-1}\rho(u)$

which shows that $t \sim u$.

Theorem 4. (Burnside)[3] $\sum_{[s]\subseteq S} 1 = \frac{1}{g}\sum_{\alpha\in\mathcal{G}} I(\alpha)$ where $I(\alpha)$ is the number of elements of S left invariant under α, where the left-hand summation is over all equivalence classes s of S and g is the order of $\mathcal{G}$.

Proof. Let $\delta_{\alpha(s),s} = \begin{cases} 1 & \text{if } \alpha(s) = s \\ 0 & \text{otherwise} \end{cases}$

Then

$$I(\alpha) = \sum_{s\in S} \delta_{\alpha(s),s}$$

We will compute the right-hand side of the theorem and prove that it is equal to the number of equivalence classes.

$$\frac{1}{g}\sum_{\alpha\in\mathcal{G}} I(\alpha) = \frac{1}{g}\sum_{\alpha\in\mathcal{G}}\sum_{s\in S} \delta_{\alpha(s),s} = \frac{1}{g}\sum_{s\in S}\sum_{\alpha\in\mathcal{G}} \delta_{\alpha(s),s}$$

$$= \frac{1}{g}\sum_{s\in S}\sum_{\substack{\alpha \\ \alpha(s)=s}} 1 = \frac{1}{g}\sum_{s\in S} h$$

where h is the order of $\mathcal{H}_s$.

$$\frac{1}{g}\sum_{s\in S} h = \frac{1}{g}\sum_{[s]\subseteq S}\sum_{s\in[s]} h = \sum_{[s]\subseteq S}\frac{1}{g}\sum_{s\in[s]} h$$

$$= \sum_{[s]\subseteq S} 1 \sum \frac{1}{g} h\,[\mathcal{G}:\mathcal{H}_s] = \sum_{[s]\in S} 1$$

The lemma was needed in the last line of this proof.

The disadvantage of the above approach is that it requires one to compute $I(\alpha)$ for every $\alpha \in \mathcal{G}$. Many of the groups to be considered have large orders and this requires considerable calculation. An even more serious restriction is that the calculation of $I(\alpha)$ is time consuming for a set of large cardinality.

There is one simplification that can be noted immediately which reduces the enumeration of all elements of $\mathcal{G}$ to the enumeration of one element from each conjugate class of $\mathcal{G}$.

Theorem 5. *If α and β are conjugates in $\mathcal{G}$, then $I(\alpha) = I(\beta)$.*

Proof. It is clearly sufficient to show that if $\alpha = \gamma^{-1}\beta\gamma$, then $\alpha(s) = s$ iff $\beta(s) = s$. Assuming $\alpha = \gamma^{-1}\beta\gamma$ and that $\alpha(s) = s$, then

$$\begin{aligned} \alpha(s) &= s = \gamma^{-1}\beta\gamma(s) \\ \gamma(s) &= \beta\gamma(s) \\ \gamma\,\gamma^{-1}(s) &= \beta(s) = s \end{aligned}$$

This set of relations shows that $I(\alpha) \leq I(\beta)$ and by the symmetry of α and β, $I(\beta) \leq I(\alpha)$ which completes the proof.

As a corollary, note that Burnside's formula now reduces to the following:

Corollary 6. $\sum_{[s] \subseteq S} 1 = \frac{1}{g} \sum_{c} n_c\, I(c)$ *where n_c is the cardinality of conjugate class c; $I(c)$ is the number of elements of S invariant under any one element of c. The sum is over all classes.*

This formula is the one employed by Slepian in references [40] [41], and by Davis [6].

The technique to be used in the present work is due originally to Pólya. The development of this theorem rests ultimately on Burnside's theorem, but the Pólya formulation is quite general. Since the applications will eventually be to Boolean functions, the statement of the theorem is formulated in terms of arbitrary functions from a finite domain to a finite range. This formulation will make it possible to relate some generalizations of DeBruijn [7] to the present discussion.

Let F be the class of all functions from a finite set D to a finite set R. Suppose D has s elements and that $\mathcal{G}$ is a permutation group of degree s and order g acting on D. Two functions f_1, $f_2 \in F$ are called equivalent if and only if there exists a permutation $\alpha \in \mathcal{G}$ such that $f_1(d) = f_2(\alpha(d))$ for all $d \in D$. Consider $R(\bar{R}=q)$ to be represented as the union of r disjoint subsets, i.e., $R = \bigcup_{i=1}^{r} R_i$ and $R_i \cap R_j = \emptyset$ if $i \neq j$. Let $k_1,\ldots,k_r$ be a partition of s. Polya's theorem tells us the number of equivalence classes of functions from D to R such that for k_i values of $d \in D$, the image $f(d) \in R_i$ for $i=1,\ldots,r$.

The numbers that are to be derived cannot in general be given by a closed form expression. An alternative is to express the numbers as the coefficients of an infinite series. For instance, a convenient closed form expression for the number of partitions of n is not known, but it is known that this number p(n) is the coefficient of x^n in the series given by

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{i=1}^{\infty} (1 - x^i)^{-1}$$

Polya's theorem is given in terms of generating functions. By a generating function is meant a polynomial in several indeterminates whose coefficients are the numbers of interest. Since the indeterminates are to be thought of as simply symbols rather than variables ranging over the complex numbers, no questions of existence or convergence ever arise.

To every set R_i, an indeterminate x_i is attached and ψ_i is the number of elements in R_i for $i=1,\ldots,r$. The figure counting series is defined as $\Psi(x_1,\ldots,x_r) = \sum_{i=1}^{r} \psi_i x_i$

Usually the convention is adopted of taking $x_1=1$. Let $P(x_1,\ldots,x_r)$ be the multi-variate generating function of these desired numbers, that is, the coefficient of $x_1^{k_1}\ldots x_r^{k_r}$ is the number of classes of functions with the property that for k_i values of $d \in D$, $f(d) \in R_i$ where $i=1,\ldots,r$. $P(x_1,\ldots,x_r)$ is often called the configuration counting series.

Before stating Polya's theorem, we must develop the concept of the cycle index polynomial of $\mathcal{J}$ (Zyklenzeiger), denoted by $Z_{\mathcal{J}}$. Let $f_1,\ldots,f_s$ be s indeterminates, and let $g_{j_1,j_2,\ldots,j_s}$ be the number of permutations of $\mathcal{J}$ having j_i cycles of length i for $i=1,2,\ldots,s$, so that

$$\sum_{i=1}^{s} ij_i = s \qquad (1)$$

Then we define

$$Z_{\mathcal{G}} = \frac{1}{g} \sum_{(j)} g_{j_1,j_2,\ldots,j_s} f_1^{j_1} f_2^{j_2} \ldots f_s^{j_s}$$

where the sum is taken over all partitions of s which satisfy (1).

Now Pólya's theorem can finally be stated; this theorem reduces the problem of determining the number of equivalence classes to the determination of the figure counting series and the cycle index polynomial.

Theorem 7. (Pólya). The configuration counting series is obtained by substituting the figure counting series into the cycle index polynomial of $\mathcal{G}$.

$$P(x_1,\ldots,x_r) = Z_{\mathcal{G}}(\psi(x_1,\ldots,x_r),\psi(x_1^2,\ldots,x_r^2),\ldots,\psi(x_1^s,\ldots,x_r^s))$$

Proof. Let $k_1,\ldots,k_r$ be a partition of s and let $\gamma \in \mathcal{G}$. $I_{k_1,\ldots,k_r}(\gamma)$ denotes the number of functions invariant under γ such that for k_i values of $d \in D$, $f(d) \in R_i$ for $i=1,\ldots,r$. Let $p_{k_1,\ldots,k_r}$ denote the number of equivalence classes with this property and note that $p_{k_1,\ldots,k_r}$ is the coefficient of $x_1^{k_1}\ldots x_r^{k_r}$ in $P(x_1,\ldots,x_r)$. By Burnside's result,

$$p_{k_1,\ldots,k_r} = \frac{1}{g} \sum_{\alpha \in \mathcal{G}} I_{k_1,\ldots,k_r}(\gamma)$$

The problem is now to find

$$\chi_\gamma(x_1,\ldots,x_r) \triangleq \sum_{k_1} \ldots \sum_{k_r} I_{k_1,\ldots,k_r}(\gamma)\, x_1^{k_1}\ldots x_r^{k_r}$$

Consider a function f such that a cycle $(d_1,\ldots,d_\ell)$ where $d_i \epsilon D$ for $i=1,\ldots,\ell$ of length ℓ leaves f invariant. All the $d_i (i=1,\ldots,\ell)$ must map into the same R_i since $(d_1,\ldots,d_\ell)$ f=f. The figure counting series for functions invariant under cycles of length ℓ is

$$\psi^{\ell}(x_1^{\ell},\ldots,x_r^{\ell}) = \sum_{i=1}^{r} \psi_i \, x_i^{\ell}$$

Let $\gamma \epsilon \mathcal{O}_j$ have j_i cycles of length i for i=1,...,s. Because the cycles are disjoint,

$$\chi_\gamma(x_1,\ldots,x_r) = \psi^{j_1}(x_1,\ldots,x_r)\,\psi^{j_2}(x_1^2,\ldots,x_r^2)\cdots\psi^{j_s}(x_1^s,\ldots,x_r^s)$$

$$= \prod_{i=1}^{s} \psi^{j_i}(x_1^i,\ldots,x_r^i)$$

Now combining the results

$$P(x_1,\ldots,x_r) = \sum_{k_1}\cdots\sum_{k_r} p_{k_1,\ldots,k_r}\, x_1^{k_1}\cdots x_r^{k_r}$$

$$= \sum_{k_1}\cdots\sum_{k_r} \frac{1}{g}\sum_{\gamma\epsilon\mathcal{O}_j} I_{k_1,\ldots,k_r}(\gamma)\, x_1^{k_1}\cdots x_r^{k_r}$$

$$= \frac{1}{g}\sum_{\gamma\epsilon\mathcal{O}_j}\sum_{k_1}\cdots\sum_{k_r} I_{k_1,\ldots,k_r}(\gamma)\, x_1^{k_1}\cdots x_r^{k_r}$$

$$= \frac{1}{g}\sum_{\gamma\epsilon\mathcal{O}_j}\chi_\gamma(x_1,\ldots,x_r)$$

$$= \frac{1}{g}\sum_{\gamma\epsilon\mathcal{O}_j}\prod_{i=1}^{s}\psi^{j_i}(x_1^i,\ldots,x_r^i)$$

$$= Z_{\mathcal{O}_j}(\psi(x_1,\ldots,x_r),\psi(x_1^2,\ldots,x_r^2),\ldots,\psi(x_1^s,\ldots,x_r^s)).$$

There is one part of the definition of the cycle index of $\mathcal{G}$ which is somewhat arbitrary. The polynomial has been defined as a sum over all partitions of s. The crucial point is only that the polynomial must be summed over all elements in $\mathcal{G}$. Sometimes it will be convenient to sum over conjugate classes and sometimes over partitions of s. In special cases, these two sets can be the same, but generally they are different.

One should note that the sum of the products of the exponents and subscripts in each term is s, since this sum is just the partitions over which the cycle index is generally summed. Also it is a convenient check to take $f_i=1$ for $i=1,\ldots,s$. The value of the cycle index should then be unity.

The cycle index polynomial contains all the information about the structure of $\mathcal{G}$ as a permutation group. Since this structure is essential to all calculations involving the number of classes induced by $\mathcal{G}$, one might suspect that the cycle index will be the foundation of all the arguments. This suspicion will prove to be correct.

The problems to be investigated in the program will require an extended definition of equivalence. In addition to $\mathcal{G}$ acting on D, let a group $\mathcal{H}$ of degree q act on R. Then one defines $f_1 \sim f_2$ iff $(\exists \alpha)$ $(\exists \beta)$ $f_1(\alpha(d)) = \beta f_2(d)$ for every $d \in D$. Now the determination of the classes poses an even more complicated problem than before. A new formula for counting the number of classes will be derived. This theorem is a special case of both DeBruijn's [7] theorems 1 and 2. The proof given here is original.

Lemma 8. $\sum_{[f]\subseteq F} 1 = \frac{1}{g}\frac{1}{h}\sum_{\alpha\in \mathcal{G}}\sum_{\beta\in \mathcal{H}} I(\alpha,\beta)$ where $I(\alpha,\beta)$ is the number of functions with the property that $f(\alpha(d)) = \beta f(d)$.

Proof. This lemma is reduced to Burnside's theorem by taking S to be the set of functions F and the group to be the direct product $\mathcal{G}\times\mathcal{H}$. It is important to note (for later purposes) that domain and range transformations commute.

Now the appropriate theorem of DeBruijn[7] may be stated.

Theorem 9. $\sum_{[f]\subseteq F} 1 = Z_{\mathcal{G}}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_s}\right) Z_{\mathcal{H}}(h_1,\ldots,h_q)$ where

$$h_t = \exp\left(\sum_{k=1}^{s/t} t z_{kt}\right) \quad \text{for } t=1,\ldots,q$$

Proof. The problem is to evaluate $I(\alpha,\beta)$. Assume α has b_i cycles of length i for i=1,...,s; suppose that β has c_i cycles of length i for i=1,...,q. Attention will now be focussed on one cycle for each permutation, say a cycle α_1 of length m for α and a cycle β_1 of length n for β. Consider a function f such that $f(\alpha_1(d)) = \beta_1 f(d)$. For this f, f(d) must be in one and the same block C of R for every $d\in B$, for if this were not the case, then f would not be invariant. It will be shown that

$$n \mid m$$

To show this, assume that $m = nq + r$ where $0 \leq r < n$. Since

$$f(\alpha_1(d)) = \beta_1 f(d)$$

it must be that

$$f(\alpha_1^m(d)) = \beta_1^m f(d).$$

This last fact is trivial to prove by induction on m. Then

$$f(\alpha_1^m(d)) = f(d) = \beta_1^{nq+r} f(d) = \beta_1^r f(d)$$

which implies that $\beta_1^r = 1$. This contradicts the definition of n as the order (or length) of β_1 unless r=0.

Thus, as d runs through any block B of length m in D, then f(d) runs through a block C of R of length n exactly $\frac{m}{n}$ times. All the invarient functions are obtained as follows. For every block B of D, associate all blocks C of R whose lengths divide the length of B. There is still the possibility of assigning an arbitrary element of C to some fixed element of B. Once this has been done, the images of all other elements of B are fixed by the requirement.

$$f(d) = r \Rightarrow f(\alpha d) = \beta r$$

Finally $I(\alpha,\beta)$ is computed

$$I(\alpha_1,\beta_1) = \prod_{\ell=1}^{s}\left(\sum_{\substack{i|\ell \\ i\leq q}} i\, c_i\right)^{b_\ell}$$

That is for every block B of D, sum the number of elements in every block C of R whose length divides the length of B. Note that

$$\prod_{\ell=1}^{s}\left(\sum_{\substack{i|\ell \\ i\leq q}} i\, c_i\right)^{b_\ell} = \frac{\partial^{b_1}}{\partial z_1^{b_1}} \cdots \frac{\partial^{b_s}}{\partial z_s^{b_s}} \exp\left(\sum_{\ell=1}^{s} z_\ell \sum_{\substack{i|\ell \\ i\leq q}} i\, c_i\right)$$

evaluated at $z_1 = \ldots = z_s = 0$. This is easily proven by taking partial derivatives. Now the results can be combined

$$\sum_{[f]\subseteq F} 1 = \frac{1}{g}\frac{1}{h}\sum_{\alpha\in\mathcal{O}_f}\sum_{\beta\in\mathcal{H}_g} I(\alpha,\beta)$$

$$= \frac{1}{g}\sum_{\alpha\in\mathcal{O}_f}\frac{\partial^{b_1}}{\partial z_1^{b_1}}\cdots\frac{\partial^{b_s}}{\partial z_s^{b_s}}\frac{1}{h}\sum_{\beta\in\mathcal{H}_g}\exp\left(\sum_{\ell=1}^{s} z_\ell \sum_{\substack{i\mid\ell\\ i\le q}} i\,c_i\right)$$

$$= Z_{\mathcal{O}_f}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_s}\right)\frac{1}{h}\sum_{\beta\in\mathcal{H}_g}\exp\left(\sum_{\ell=1}^{s} z_\ell \sum_{\substack{i\mid\ell\\ i\le q}} i\,c_i\right)$$

Note that

$$\exp\left(\sum_{\ell=1}^{s} z_\ell \sum_{\substack{i\mid\ell\\ i\le q}} i\,c_i\right) = \exp\left(\sum_{i=1}^{q} i\,c_i \sum_{k=1}^{s/i} z_{ki}\right)$$

$$= \prod_{i=1}^{q}\exp\left(i\sum_{k=1}^{s/i} z_{ki}\right)^{c_i}$$

$$\sum_{[f]\subseteq F} 1 = Z_{\mathcal{O}_f}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_s}\right)\frac{1}{h}\sum_{\beta\in\mathcal{H}_g}\exp\left(\sum_{\ell=1}^{s} z_\ell \sum_{\substack{i\mid\ell\\ i\le q}} i\,c_i\right)$$

$$= Z_{\mathcal{O}_f}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_s}\right)\frac{1}{h}\sum_{\beta\in\mathcal{H}_g}\prod_{i=1}^{q}\exp\left(i\sum_{k=1}^{s/i} z_{ki}\right)^{c_i}$$

$$= Z_{\mathcal{O}_f}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_s}\right) Z_{\mathcal{H}_g}(h_1,\ldots,h_q)$$

where $h_t = \exp\left(t\sum_{k=1}^{s/t} kt\right)$ for $t=1,\ldots,q$ and the function is evaluated

at $z_1 = \ldots = z_s = 0$. QED

Many times, one is interested in special classes of functions rather than an entire family. One class of functions of particular interest is the one-to-one onto functions or invertible functions. A new derivation of a theorem of DeBruijn[7] for calculating the number of equivalence classes of functions from D onto D will now be presented.

Theorem 10. The number of classes of invertible functions from D onto D with a group $\mathcal{J}$ on the domain and a group $\mathcal{H}$ on the range is given by

$$Z_{\mathcal{J}}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_s}\right) Z_{\mathcal{H}}(1 + z_1, \ldots, 1 + sz_s)$$

Proof. Again, Burnside's theorem may be used. It is necessary to evaluate $I'(\alpha,\beta)$ for $\alpha \in \mathcal{J}$ and $\beta \in \mathcal{H}$ remembering to count only those orbits which contain one-to-one functions.

Consider the mapping $f \to f^{-1}$ which also sends $(f^{-1}) \to (f^{-1})^{-1} = f$. This map is one-to-one and indicates to us that the number of classes with $\mathcal{J}$ on the domain and $\mathcal{H}$ on the range is the same as with $\mathcal{H}$ on the domain and $\mathcal{J}$ on the range.

Consider a cycle of α of length m and a cycle of β of length n. By the previous proof of DeBruijn's theorem,

$$n \mid m.$$

By the symmetry noted above, $m \mid n$ and so $m=n$. Thus $b_i = c_i$ for $i=1,\ldots,s$ and the determination of $I'(\alpha,\beta)$ is now trivial because this expression is now simply the number of permutations having b_i cycles of length $i(i=1,\ldots,s)$. This number is well known[42] to be

$$I'(\alpha,\beta) = \prod_{i=1}^{s} c_i!\, i^{b_i}$$

Note that this is also

$$\prod_{i=1}^{s} c_i!\, i^{b_i} = \frac{\partial^{b_1}}{\partial z_1^{b_1}} \cdots \frac{\partial^{b_s}}{\partial z_1^{b_s}} \prod_{j=1}^{s} (1 + jz_j)^{c_j}$$

evaluated at $z_1 = \ldots = z_s = 0$. Now

$$\sum_{\substack{[f] \subseteq F \\ f\ 1\text{-}1}} 1 = \frac{1}{g}\frac{1}{h} \sum_{\alpha \in \sigma_j} \sum_{\beta \in \tau_k} I'(\alpha,\beta)$$

$$= \frac{1}{g}\frac{1}{h} \sum_{\alpha \in \sigma_j} \sum_{\beta \in \tau_k} \prod_{i=1}^{s} i^{b_i} c_i!$$

$$= \frac{1}{g} \sum_{\alpha \in \sigma_j} \frac{\partial^{b_1}}{\partial z_i^{b_1}} \cdots \frac{\partial^{b_s}}{\partial z_s^{b_s}} \frac{1}{h} \sum_{\beta \in \tau_k} \prod_{i=1}^{s} (1 + i\, z_i)^{c_i}$$

$$= Z_{\sigma_j}\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_s}\right) Z_{\tau_k}(1 + z_1, \ldots, 1 + sz_s)$$

evaluated at $z_1 = \ldots = z_s = 0$.

2-2. Structure Theory For Permutation Groups

A major portion of research in mathematics is concerned with finding the structure of abstract systems. This usually means finding a well-defined class of subsystems and constructing larger systems from these simple ones by appropriate operations. This type of theory is well developed for abstract groups, but our applications require some knowledge of a similar theory for permutation groups. Unfortunately, a well developed theory of this type does not exist as yet.

The concept of equivalence between groups which we shall need is known as permutational equivalence. Permutation groups $\mathcal{G}$ and $\mathcal{H}$ on disjoint object sets X and Y are called <u>permutationally equivalent</u> if and only if $\mathcal{G}$ and $\mathcal{H}$ are isomorphic as abstract groups and there is a one-to-one correspondence h: $X \leftrightarrow Y$ such that if φ is the abstract isomorphism between $\mathcal{G}$ and $\mathcal{H}$, then for every $x \in X$, $\alpha \in \mathcal{G}$, we have $h(\alpha\, x) = (\varphi\alpha)h(x)$. Thus, two groups may be isomorphic as abstract groups but not permutationably equivalent. Note that the degree is one invariant of permutationally equivalent groups.

We shall now give some of the operations on permutation groups. In each case, it would be desirable to be able to find the cycle index of the new group in terms of the cycle indices of the two given groups.

Consider two groups $\mathcal{G}$ and $\mathcal{H}$ on disjoint object sets X and Y such that the order of $\mathcal{G}$ is m and the order of $\mathcal{H}$ is h; the degree of $\mathcal{G}$ is a and the degree of $\mathcal{H}$ is b.

The direct sum of $\mathcal{G}$ and $\mathcal{H}$ written $\mathcal{G} + \mathcal{H}$ has $X \times Y$ as its object set. The group is obtained as $\{\alpha\beta \mid \alpha \in \mathcal{G},\ \beta \in \mathcal{H}\}$. Thus we

take $\alpha\beta(z)$ = $\begin{cases} \alpha(z) & \text{if } z \in X \\ \beta(z) & \text{if } z \in Y. \end{cases}$

It is clear that the order of $\mathcal{A} + \mathcal{B}$ is mn and the degree is a + b. Pólya[30] has shown that $Z_{\mathcal{A}+\mathcal{B}} = Z_{\mathcal{A}} \; Z_{\mathcal{B}}$ where we mean the Cauchy product of polynomials by this notation.

The direct product of two groups written $\mathcal{A} \times \mathcal{B}$ is defined on the object set X x Y in the following way $(\alpha,\beta)(x,y) = (\alpha(x), \beta(y))$. Thus, the order of $\mathcal{A} \times \mathcal{B}$ is mn and the degree is ab. The groups $\mathcal{A} \times \mathcal{B}$ and $\mathcal{A} + \mathcal{B}$ are isomorphic as abstract groups but are not permutationally equivalent since they have different degrees. We shall now establish the connection between the cycle indices of $\mathcal{A}$ and $\mathcal{B}$ and the cycle index of $\mathcal{A} \times \mathcal{B}$. Let

$$Z_{\mathcal{A}} = \frac{1}{m} \sum_{(j)} c_{(j)} \, g_1^{j_1} \cdots g_a^{j_a}$$

and let

$$Z_{\mathcal{B}} = \frac{1}{n} \sum_{(k)} d_{(k)} \, h_1^{k_1} \cdots h_b^{k_b}.$$

The following theorem was stated by Harary[16].

Theorem 1. $Z_{\mathcal{A} \times \mathcal{B}} = Z_{\mathcal{A}} \times Z_{\mathcal{B}}$ <u>where the cross operation for polynomials is defined as follows</u>

$$Z_{\alpha \times \beta} = \frac{1}{m}\frac{1}{n} \sum_{(j)} \sum_{(k)} c_{(j)}\, d_{(k)} \left(\prod_{p=1}^{a} g_p^{j_p} \right) \times \left(\prod_{q=1}^{b} h_q^{k_q} \right)$$

where the cross operation on indeterminates is defined as

$$\left(\prod_{p=1}^{a} g_p^{j_p} \right) \times \left(\prod_{q=1}^{b} h_q^{k_q} \right) = \prod_{p=1}^{a} \prod_{q=1}^{b} g_p^{j_p} \times h_q^{k_q}$$

$$= \prod_{p=1}^{a} \prod_{q=1}^{b} f^{j_p k_q (p,q)}_{\langle p,q \rangle}$$

where $\langle p,q \rangle$ denotes the least common multiple of p and q while (p,q) means the greatest common divisor of p and q.

The statement of this theorem involves a certain amount of notation. For this reason, a simple example is presented. Let

$$Z_{\mathcal{S}_2} = \frac{1}{2}(g_1^2 + g_2)$$

and

$$Z_{\mathcal{S}_3} = \frac{1}{6}(h_1^3 + 3h_1h_2 + 2h_3)$$

be the cycle indices for the symmetric group on two and three letters respectively. We compute

$$Z_{\mathcal{G}_2 \times \mathcal{G}_3} = \frac{1}{12}\,(g_1^2 \times h_1^3) + 3(g_1^2 \times h_1 h_2) + 2(g_1^2 \times h_3)$$

$$+ (g_2 \times h_1^3) + 3(g_2 \times h_1 h_2) + 2(g_2 \times h_3)$$

$$= \frac{1}{12}\,(f_1^6 + 3(g_1^2 \times h_1)(g_1^2 \times h_2) + 2f_3^2 + f_2^3$$

$$+ 3(g_2 \times h_1)(g_2 \times h_2) + 2f_6)$$

$$= \frac{1}{12}\,(f_1^6 + 3f_1^2 f_2^2 + 2f_3^2 + 4f_2^3 + 2f_6)$$

Before leaving this example, it is interesting to note that this example solves a nontrivial problem of graph theory. If one substitutes $1 + x^i$ for f_i in $Z_{\mathcal{G}_2 \times \mathcal{G}_3}$ then the coefficient of x^q is the number of chromatically nonisomorphic spanning subgraphs of the complete graph K_{23} having q lines cf. Harary [16].*

Proof. It is easily verified that the cross operation on indeterminites is associative, commutative, and distributive over addition. It will be sufficient to examine the cycle structure of (α,β) where α is a cycle of length p, say $(a_1,\ldots,a_p)$ and β is a cycle of length q say $(b_1,\ldots,b_q)$. The case p=q is trivial so we assume $p<q$. Examining an element $(a_1,b_1) \in X \times Y$ we see that (a_1,b_1) goes successively into $(a_2,b_2),(a_3,b_3),\ldots,(a_p,b_p),(a_1,b_{p+1}),\ldots$; we return to (a_1,b_1) after

---

* Roughly speaking, a graph is colored if its vertices are painted so that no two adjacent vertices have the same color. Two graphs are chromatically isomorphic iff the uncolored graphs are isomorphic and the colored of the graphs can be made to correspond via a permutation which is consistent with respect to the isomorphism. The precise definition of these concepts occurs in Chapter 5.

$\langle p,q\rangle$ steps and the pq symbols are permuted in (p,q) steps of length $\langle p,q\rangle$. Recall that $pq = \langle p,q\rangle(p,q)$. The argument is completed by noting that the choice of a_1 and b_1 is arbitrary; any pair of elements one in α and one in β would have given the same result.

Another operation of importance is the wreath product or Kranzgruppen of Pólya[30], denoted by $\mathcal{S}_\mathcal{B} \wr \mathcal{A}$ in the modern notation (cf. Hall[14]). This group has as its object set $X \times Y$; a convenient formulation is to consider the object set to be a matrix (x_{ij}) with a rows and b columns. The operations are defined by first permuting the rows by an operation of $\mathcal{A}$ and then permuting the column indices in each of the a rows separately by an element of $\mathcal{S}_\mathcal{B}$ allowing repetitions. The order of this group is seen to be mn^a since there are m choices for the element of $\mathcal{A}$ and n choices for each of the a elements of $\mathcal{S}_\mathcal{B}$. Some observations about this group will prove useful. Note that $\mathcal{A}$ is a subgroup of $\mathcal{S}_\mathcal{B} \wr \mathcal{A}$ obtained by always choosing the n^a elements of $\mathcal{S}_\mathcal{B}$ to all be the identity. We also note that $\mathcal{S}_\mathcal{B} \times \ldots \times \mathcal{S}_\mathcal{B}$ is another subgroup obtained by taking the identity operation in $\mathcal{A}$. This last subgroup is seen to be normal in $\mathcal{S}_\mathcal{B} \wr \mathcal{A}$, so that

$$\mathcal{S}_\mathcal{B} \wr \mathcal{A} \Big/ \mathcal{S}_\mathcal{B} \times \cdots \times \mathcal{S}_\mathcal{B} \cong \mathcal{A}$$

Now we turn our attention to getting the pertinent result about the cycle index of $\mathcal{S}_\mathcal{B} \wr \mathcal{A}$. Let

$$Z_{\mathcal{A}} = \frac{1}{m} \sum_{(j)} c_{(j)} g_1^{j_1} \cdots g_a^{j_a}$$

and

$$Z_{\mathcal{G}} = \frac{1}{b} \sum_{(k)} d_{(k)} \, h_1^{k_1} \cdots h_b^{k_b}.$$

Theorem 2. (Pólya) $Z_{\mathcal{G} \wr \mathcal{H}} = Z_{\mathcal{H}}[Z_{\mathcal{G}}]$

$$= \frac{1}{m} \sum_{(j)} c_{(j)} \, z_1^{j_1} \cdots z_a^{j_a}$$

where

$$z_p = \frac{1}{n} \sum_{(k)} d_{(k)} \, h_{p1}^{k_1} \cdots h_{pb}^{k_b} \quad \text{for } p=1,\ldots,a.$$

Proof. The result is fairly clear from the construction but the details are to be found in Pólya[30].

Example. The cycle index of $\mathcal{S}_2 \wr \mathcal{S}_3$ is now computed.

$$Z_{\mathcal{S}_2 \wr \mathcal{S}_3} = \left(\frac{1}{6}\left(\frac{1}{2}(f_1^2 + f_2)\right)^3 + 3\left(\frac{1}{2}(f_1^2 + f_2)\right)\left(\frac{1}{2}(f_2^2 + f_4)\right) + 2\frac{1}{2}(f_3^2 + f_6) \right)$$

$$= \frac{1}{48}\left(f_1^6 + 3f_1^4 f_2 + 3f_1^2 f_2^2 + f_2^3 + 6(f_1^2 f_2^2 + f_1^2 f_4 + f_2^3 + f_2 f_4) + 8f_3^2 + 8f_6 \right)$$

$$= \frac{1}{48}\left(f_1^6 + 3f_1^4 f_2 + 9f_1^2 f_2 + 9f_2^3 + 6f_1^2 f_4 + 6f_2 f_4 + 8f_3^2 + 8f_6 \right)$$

It is no accident that the result is the cycle index of the symmetry group of the three-dimensional octehedron.

Another operation of importance for our application is that of exponentiation of permutation groups. Harary[15] originally constructed

this operation in order to systematize the calculations which Slepian[40] had made in his work on Boolean functions. For this purpose, Harary's definition is unfortunate. At this time a more appropriate definition of exponentiation is presented; a new type of product will be discussed later which will characterize exactly what Slepian did. Harary's definition and its consequences are given in appendix V.

The exponentiation of $\mathcal{M}$ and $\mathcal{G}$ is written $\mathcal{G}^{\mathcal{M}}$ and has as its object set Y^X, the class of all functions from X into Y. An element in $\mathcal{G}^{\mathcal{M}}$, say $\beta\alpha$, operates on these functions in the following way $\beta\alpha f(d) = \beta f(\alpha(d))$. It is clear that any α and β commute so that the order of $\mathcal{G}^{\mathcal{M}}$ is mn and the degree is b^a. It should be noted that this situation is exactly the same as the one we analysed in proving the DeBruijn theorems. It will not be necessary to consider the construction of $Z_{\mathcal{G}^{\mathcal{M}}}$ since we already have these results concerning the number of classes.

Harary[15] has investigated some of the inter-relations between the family of permutation groups and these operations on them. We restate his theorem now.

Theorem 3.

a. The family of all permutation groups is closed under the operations previously defined.

b. If we let $\mathcal{I}_0$ be the group of degree 0 and order 1; $\mathcal{I}_1$ be the group of degree and order 1, then for any permutation group $\mathcal{M}$,

$$\mathcal{A} + \mathcal{I}_0 = \mathcal{A}$$

$$\mathcal{A} \times \mathcal{I}_1 = \mathcal{A}$$

$$\mathcal{I}_1 \wr \mathcal{A} = \mathcal{A} = \mathcal{A} \wr \mathcal{I}_1$$

$$\mathcal{A}^{\mathcal{I}_1} = \mathcal{A}$$

c. For any permutation groups $\mathcal{A}$ and $\mathcal{B}$

$$\mathcal{A} + \mathcal{B} = \mathcal{B} + \mathcal{A}$$

$$\mathcal{A} \times \mathcal{B} = \mathcal{B} \times \mathcal{A}$$

d. For any permutation groups $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$

$$\mathcal{A} + (\mathcal{B} + \mathcal{C}) = (\mathcal{A} + \mathcal{B}) + \mathcal{C}$$

$$\mathcal{A} \times (\mathcal{B} \times \mathcal{C}) = (\mathcal{A} \times \mathcal{B}) \times \mathcal{C}$$

$$\mathcal{C} \wr (\mathcal{B} \wr \mathcal{A}) = (\mathcal{C} \wr \mathcal{B}) \wr \mathcal{A}$$

e. The only distributive law which can hold between these groups under the operations of wreath product, sum, and product is

$$\mathcal{C} \wr (\mathcal{A} + \mathcal{B}) = (\mathcal{C} \wr \mathcal{A}) + (\mathcal{C} \wr \mathcal{B})$$

A new group product will be formulated which will characterize Slepian's result[40] and will find applications in a variety of situations. Let $\mathcal{B}$ be a group of order g acting on object set X. The degree of $\mathcal{B}$ is assumed to be b. Let $\mathcal{A}$ be a group of order m

acting on a copies of X; thus, the degree of $\mathcal{A}$ is b^a. A new group $\mathcal{A} \otimes \mathcal{B}$ will now be defined. It is convenient to think of a-tuples of X^a listed. If the array is thought of as a matrix of a columns and b^a rows, then the operations of $\mathcal{A} \otimes \mathcal{B}$ are constructed by first selecting $\alpha \in \mathcal{A}$ which causes a permutation of the rows of the matrix. Selecting elements $\beta_1, \ldots, \beta_a$ from $\mathcal{B}$ (not necessarily distinct), the i^{th} column is to be permuted by β_i for $i=1,\ldots,a$. Thus, $\mathcal{A} \otimes \mathcal{B}$ is easily seen to be a group isomorphic to $\mathcal{B} \wr \mathcal{A}$ but not permutationally equivalent to it. The abstract structure of $\mathcal{A} \otimes \mathcal{B}$ is the semi-direct product of $\mathcal{A}$ by $\mathcal{B}^a$ where $\mathcal{B}^a$ denotes $\mathcal{B} \times \ldots \times \mathcal{B}$.

Now we turn to the problem of computing $Z_{\mathcal{A} \otimes \mathcal{B}}$ in terms of $Z_{\mathcal{A}}$ and $Z_{\mathcal{B}}$. The following exhaustive (and exhausting) procedure will work for computing $Z_{\mathcal{A} \otimes \mathcal{B}}$ when enumeration is possible. Write out all possible permutations of $\mathcal{A}$ and all possible permutations of $\mathcal{B}^a$. Compose the permutations and write down the cycle structures. This procedure suffers from some of the defects of the Burnside approach to enumeration. In general, the problem of finding $Z_{\mathcal{A} \otimes \mathcal{B}}$ in terms of $Z_{\mathcal{A}}$ and $Z_{\mathcal{B}}$ is still unsolved. An algorithm is now given when $\mathcal{A}$ is the symmetric group on the n columns and hence a group $\mathcal{S}_n$ is induced as a permutation group on the rows.

In the case described where $\mathcal{A}$ is the symmetric group, $\mathcal{S}_n \times \mathcal{B}$ has the abstract structure of the complete monomial group of degree n of $\mathcal{B}$. The theory of such groups has been worked out by Ore[28] and reference to several of his theorems will be made. For the purposes of this thesis, it will be sufficient to derive the cycle index of $\mathcal{S}_n \otimes \mathcal{B}$ where $\mathcal{B}$ has a restricted type of cycle

structure. The condition on $\mathcal{G}$ can be expressed by requiring that $Z_{\mathcal{G}}$ is of the form

$$Z_{\mathcal{G}} = \frac{1}{g} \sum_{(k)} b_{(k)} f_k^s.$$

Although the restrictions imposed on $\mathcal{G}$ are severe, it is surprising that the results obtained have wide applicability.

The formula is now presented. Since the result is complicated, the reader will wish to read chapter three before examining the proof of theorem 4. For the reason the proof is given in appendix VI.

Theorem 4. *Let γ_n be the group induced by the symmetric group of degree n and let $\mathcal{G}$ be a group of degree m and order g whose cycle index has terms whose structure is of the form f_k^s.*

$$Z_{\gamma_n \otimes \mathcal{G}} = \frac{1}{n!} \sum_{(j)} \frac{n!}{\prod_{i=1}^{n} j_i!\, i^{j_i}} \prod_{i=1}^{n} \left(\frac{1}{g} \sum_{(k)} b_{(k)} \prod_{\substack{d \mid ik \\ d \nmid pi \\ p<k}} f_d^{e_i(d)} \right)^{x^{j_i}}$$

where $e_i(d)$ can be computed recursively from the following relation

$$\sum d\, e_i(d) = m^k$$

where the sum is over the same set as the product in the formula for $Z_{\gamma_n \otimes \mathcal{G}}$.

Proof. The theorem is proven in appendix VI.

We shall conclude the section by remarking that surprisingly many groups satisfy the hypothesis on $\mathcal{S}_\sigma$.

Example. Let $\mathcal{S}_\sigma$ be the cyclic group of degree and order 3.

$$Z_{\mathcal{S}_\sigma} = \frac{1}{3}(f_1^3 + 2f_3)$$

$$Z_{\mathcal{M}_2 \otimes \mathcal{S}_\sigma} = \frac{1}{2}\left(\frac{1}{3}(f_1^3 + 2f_3)\right)^{x2} + \frac{1}{3}(f_1^3 f_2^3 + 2f_3 f_6)$$

$$= \frac{1}{18}(f_1^9 + 8f_3^3 + 3f_1^3 f_2^3 + 6f_3 f_6)$$

The group operations are shown in Table I along with the important parameters.

OPERATIONS ON PERMUTATION GROUPS

Group	$\mathcal{A}$	$\mathcal{S}$	$\mathcal{A}+\mathcal{S}$	$\mathcal{A}\times\mathcal{S}$	$\mathcal{S}\wr\mathcal{A}$	$\mathcal{S}^{\mathcal{A}}$
Object Set	X	Y	$X \cup Y$	$X \times Y$	$X \times Y$	Y^X
Degree	a	b	a+b	ab	ab	b^a
Order	m	n	mn	mn	mn^a	mn
Group	$\mathcal{A}$	$\mathcal{S}$	$\mathcal{A}^{\mu}_{a}\otimes\mathcal{S}$	$\mathcal{A}\otimes\mathcal{S}$		
Object Set	X^a	X	X^a	X^a		
Degree	b^a	b	b^a	b^a		
Order	m	n	$a!n^a$	mn^a		

TABLE I

CHAPTER III

SWITCHING FUNCTIONS AND PERMUTATION GROUPS

3-1. Introduction

We shall call functions from $\{0,1\}^n$ into $\{0,1\}$ switching or Boolean functions. The class of all such 2^{2^n} functions forms a free Boolean algebra on n generators having 2^n atoms and denoted by F_n. The reader is referred to reference [38] for the theory of Boolean algebras. We shall be interested in solving certain combinatorial problems in classifying these functions. Whenever possible, the results will be given in the most general possible form even though our applications will be only to F_n.

3-2. Groups on Functions

There are certain types of permutation groups which can be defined on Boolean functions. For instance, one might define the full permutation groups on all 2^{2^n} functions. This group on all the functions has order $2^{2^n}!$. No useful applications have yet been found for this group because the group is too large and does not preserve interesting relations between functions.

It also seems natural to define permutation groups on the domain of Boolean functions. Examination of permutations on the domain indicates an important fact, namely these permutations are exactly the automorphisms of F_n. To review the terminology briefly, a mapping h from a Boolean algebra A into a Boolean algebra B is said to be a homomorphism iff

$$h(a + b) = h(a) + h(b)$$

$$h(ab) = h(a)\, h(b)$$

and

$$h(\bar{a}) = \overline{h(a)}$$

An isomorphism is a one-to-one and onto homomorphism. An endomorphism of a Boolean algebra is a homomorphism from an algebra into itself while an automorphism is an isomorphism of Boolean algebra with itself. It is well known that the class of automorphisms of a Boolean algebra forms a group.

Theorem 1. Let A be a Boolean algebra having k atoms and 2^k elements. The automorphism group of A is exactly the group of all k! permutations of the atoms and is isomorphic to the symmetric group on k letters.

Proof. Clearly every automorphism preserves the partial order of A and hence maps minimal elements into minimal elements. Since the automorphism is one-to-one and onto, it is a permutation of the atoms. Let σ be a permutation of the atoms of A. Using the normal form expansion, we see that σ induces a mapping from A into A, i.e.

$$\sigma\colon f = \sum_{i \in I} a_i \rightarrow \sigma f = \sum_{i \in I} a_{\sigma(i)}$$

To show the onto property, note that if we are given

$$f = \sum_{i \in I} a_i$$

then the function

$$\sigma^{-1}(f) = \sum_{i\epsilon I} a_{\sigma^{-1}(i)}$$

maps onto f under σ.

Now we show that σ preserves the structure. Let $f = \sum_{i\epsilon I} a_i$ and $g = \sum_{j\epsilon J} a_j$, then

$$\sigma(f + g) = \sigma(\sum_{i\epsilon I} a_i + \sum_{j\epsilon J} a_j) = \sigma(\sum_{k\epsilon I\cup J} a_k)$$

$$= \sum_{k\epsilon I\cup J} a_{\sigma(k)} = \sum_{k\epsilon I} a_{\sigma(i)} + \sum_{j\epsilon J} A_{\sigma(j)}$$

$$= \sigma(f) + \sigma(g)$$

Similarly,

$$\sigma(fg) = \sigma(f)\,\sigma(g)$$

Lastly, we compute

$$\sigma(\bar{f}) = \sigma \sum_{i\notin I} a_i) = \sum_{i\notin I} a_{\sigma(i)} = (\overline{\sigma f})$$

Lastly, we show that σ is one-to-one. Suppose

$$\sigma f = \sigma g$$

This happens iff

$$\sigma^{-1}\,\sigma\, f = f = \sigma^{-1}\,\sigma g = g$$

Corollary 2. The automorphism group of F_n is the symmetric group on the 2^n atoms, denoted by $\mathcal{S}_{2^n}$.

It is interesting to note that the endomorphisms of a Boolean algebra can be constructed in an analogous way. It is possible to

show the endomorphisms of a Boolean algebra are exactly the mappings from the atoms into the atoms. Thus, the Boolean algebra F_n has 2^{n2^n} endomorphisms.

There is one last place that one can define a permutation group. Suppose that one defines transformations on the variables $x_1,\ldots,x_n$ of F_n. These transformations induce permutations of the atoms and hence automorphisms of F_n. The applications of Boolean functions to switching theory generally suggest natural groups to apply to the variables.

3-3. A More Precise Characterization of our Problems

The first class of problems to be investigated involves a single group on the domain. For this class of problems one need only apply Polya's theorem.

Since the range of our functions is $\{0,1\} = R$, take $R_1 = \{0\}$ and $R_2 = \{1\}$. With R_1, associate the indeterminate 1, and with R_2 associate the indeterminate x. Thus, the range enumerating series for switching functions is

$$\Psi(x) = 1 + x$$

Thus, our enumeration results for Boolean functions can be obtained by constructing the cycle index of the group under consideration. It is important to note that this group must be of degree 2^n, i.e. defined over the domain, not the set of variables.

Before proceeding to the actual constructions, a trivial case is given as an example.

Let $\mathcal{I}_n$ be the identity group on the n variables. $\mathcal{I}_n$ is of order one and induces a group on the domain of degree 2^n. The cycle index of the induced group is given by

$$Z_{\mathcal{I}_n} = f_1^{2^n}$$

Then by Polya's theorem

$$P(x) = (1 + x)^{2^n} = \sum_{i=0}^{2^n} \binom{2^n}{i} x^i$$

which says that the number of switching functions of weight k, that is, having k ones in their graph or k atoms in their normal form expansion is $\binom{2^n}{k}$. Note by taking

$$P(1) = Z_{\mathcal{I}_n}(2) = \sum_{i=0}^{2^n} \binom{2^n}{i} = 2^{2^n}$$

that we get the total number of functions. If one is merely interested in the total number of classes, take $f_i = 1 + 1^i = 2$ in $Z_{\mathcal{G}}(f_1,\ldots,f_s)$ for i=1,...,s and compute $Z_{\mathcal{G}}(2,\ldots,2)$.

3-4. The Group Σ_2^n

The first mathematical investigations of switching theory concerned the analysis of relay contact networks. In such networks, the cost of a normally closed contact is the same as the cost of a normally open contact. This suggests calling the following two networks equivalent.

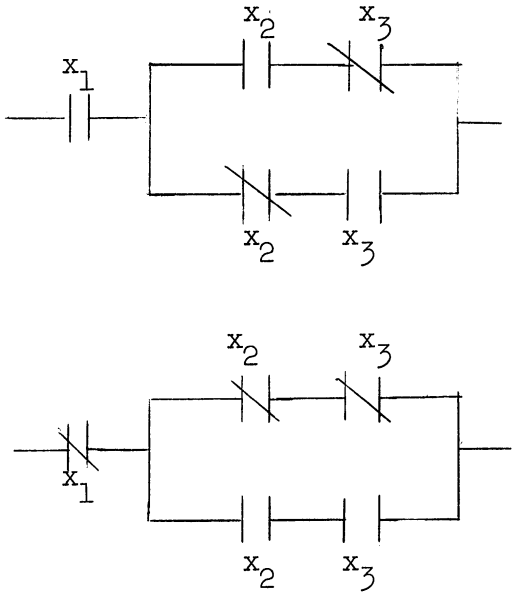

Fig. I. Two Networks Which are Equivalent Under Σ_2^3

Definition 1. The group $\Sigma_2 = \langle\{0,1\}, \oplus, 0\rangle$ is defined with the operation of addition modulo 2.

Definition 2. The symbol Σ_2^n denotes $\Sigma_2 \times \ldots \times \Sigma_2$, i.e. the abstract direct product of n copies of Σ_2. Thus, elements of Σ_2^n are n-tuples of zeroes and ones; the operation of the group is digit-wise modulo two addition. Of course, the identity element is $(0,\ldots,0)$.

Now this group is defined on Boolean functions in the same way that Ashenhurst[2] did.

Definition 3. Let $i \in \Sigma_2^n$ and let $f(x_1,\ldots,x_n)$ be a Boolean function of n variables. Define

$$if = (i_1,\ldots,i_n)\ f(x_1,\ldots,x_n) = f(x_1^{i_1},\ldots,x_n^{i_n})$$

$$\text{where } x_j^{i_j} = \begin{cases} x_j & \text{if } i_j = 0 \\ \bar{x}_j & \text{if } i_j = 1 \end{cases} \qquad \text{for } j=1,\ldots,n$$

Rather than compute the cycle index of Σ_2^n in the way that Ashenhurst did, we shall derive it from the structure of Σ_2^n as a permutation group and indicate some of the power of a structural theory of permutation groups.

Theorem 4. As a permutation group, $\Sigma_2^n = \Sigma_2 \times \ldots \times \Sigma_2$.

Proof. Consider Σ_2 defined as a permutation group on the set consisting of zero and one. Using the definition of the product of permutation groups, it is evident that $\Sigma_2^n = \Sigma_2 \times \ldots \times \Sigma_2$.

Theorem 5. $Z_{\Sigma_2^n} = \frac{1}{2^n}(f_1^{2^n} + (2^n - 1) f_2^{2^{n-1}})$

Proof. By theorem 2-2.1,

$$Z_{\Sigma_2^n} = \bigtimes_{i=1}^{n} \frac{1}{2}(f_1^2 + f_2)$$

It is claimed that

$$\bigtimes_{i=1}^{n} \frac{1}{2}(f_1^2 + f_2) = \frac{1}{2^n}(f_1^{2^n} + (2^n - 1) f_2^{2^{n-1}}).$$

To show this by induction, we need only compute

$$\frac{1}{2^{n-1}} \left(f_1^{2^{n-1}} + (2^{n-1} - 1)\, f_2^{2^{n-2}}\right) \times \frac{1}{2} \left(f_1^2 + f_2\right)$$

$$= \frac{1}{2^n} \left(f_1^{2^n} + (2^{n-1} - 1)\, f_2^{2^{n-1}} + f_2^{2^{n-1}} + (2^{n-1}-1)\, f_2^{2^{n-1}}\right)$$

$$= \frac{1}{2^n} \left(f_1^{2^n} + (2^n - 1)\, f_2^{2^{n-1}}\right)$$

Before applying this result to Boolean functions, it is interesting to note that a still stronger version of the theorem can be shown to be true, namely the following:

Theorem 6. Let $\mathcal{h}$ be the regular representator of the (abelian) group of order p^k and type $(1,\ldots,1)$ then $Z_{\mathcal{h}} = \frac{1}{p^k} \left(f_1^{p^k} + (p^k - 1)\, f_p^{p^{k-1}}\right)$ for any prime p and $k \geq 1$.

Proof. Clearly $\mathcal{h}$ has degree and order p^k. Let φ_x be any non-identity element of $\mathcal{h}$.

$$\varphi_x : a \to ax$$

All the images of φ must be in a single cycle of length p, for if they did not, there might for example be two shorter cycles, any one of length k and one of length ℓ. The argument to be presented follows for any number of cycles. Since $(k + \ell) = p$, we must have $(k,\ell) = 1$ or p since any common factor of k and ℓ divides p. Assume $(k,\ell) \neq p$ since then we would be done. Thus, we have that the order φ_x is $p = \langle k,\ell \rangle = \frac{k}{(k,\ell)} = k$ which is a contradiction unless one of k or ℓ is p. Thus, the cycle index of $\mathcal{h}$ is given by

$$Z_{\mathfrak{h}} = \frac{1}{p^k}\left(f_1^{p^k} + (p^k - 1)\, f_p^{p^{k-1}}\right)$$

Now we return to Boolean functions and begin to collect our results.

Theorem 7. The number of equivalence classes of functions having k atoms in their (unique) normal form expansion under Σ_2^n is

$$\frac{1}{2^n}\binom{2^n}{k} \text{ if } k \equiv 1 \bmod 2$$

and

$$\frac{1}{2^n}\left(\binom{2^n}{k} + (2^n - 1)\binom{2^{n-1}}{k/2}\right) \text{ if } k \equiv 0 \bmod 2$$

Proof. By Pólya's theorem,

$$Z_{\Sigma_2^n}(1 + x) = \frac{1}{2^n}\left((1 + x)^{2^n} + (2^n - 1)(1 + x^2)^{2^{n-1}}\right)$$

$$= \frac{1}{2^n}\left(\sum_{k=0}^{2^n}\binom{2^n}{k}x^k + (2^n - 1)\sum_{j=0}^{2^{n-1}}\binom{2^{n-1}}{j}x^{2j}\right)$$

If $k \equiv 1 \bmod 2$, the coefficient of x^k is $\frac{1}{2^n}\binom{2^n}{k}$.

If $k \equiv 0 \bmod 2$, the coefficient of x^k is

$$\frac{1}{2^n}\left(\binom{2^n}{k} + (2^n - 1)\binom{2^{n-1}}{k/2}\right)$$

Theorem 8. The total number of equivalence classes of Boolean functions under $\sum_2^n$ is

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

Proof. By Polya's theorem, take $f_i = 1 + 1^i = 2$ in $Z_{\sum_2^n}$.

Some typical calculations for this group have been made and the results are tabulated in Table I. We use T_n for the total number of equivalence classes and N_n^k for the number of classes of functions having k atoms in their normal form expansions. Note that $N_n^k = N_n^{2^n-k}$ which is a consequence of the law of duality for Boolean functions.

THE NUMBER OF CLASSES OF FUNCTIONS WITH k ATOMS UNDER Σ_2^n

k \ n	N_n^k 1	2	3	4	5
0	1	1	1	1	1
1	1	1	1	1	1
2	1	3	7	15	31
3		1	7	35	155
4		1	14	140	1,240
5			7	273	6,293
6			7	553	28,861
7			1	715	105,183
8			1	870	330,460
9				715	876,525
10				553	2,020,239
11				273	4,032,015
12				140	7,063,784
13				35	10,855,425
14				15	14,743,445
15				1	17,678,835
16				1	18,796,230
T_n	3	7	46	4,336	134,281,216

TABLE II

As an example of the classification of functions induced on F_2 by Υ_2^2, the equivalence classes are listed below

$$[0] \qquad\qquad [1]$$
$$[x, \bar{x}] \qquad\qquad [y, \bar{y}]$$
$$[\bar{x} + \bar{y},\ \bar{x} + y,\ x + \bar{y},\ x + y]$$
$$[\bar{x}\bar{y},\ \bar{x}y,\ x\bar{y},\ xy]$$
$$[x \oplus y,\ x \equiv y]$$

3-5. The Symmetric Group γ_n

The sort of equivalence induced on functions by Υ_2^n has practical significance because the intended applications were to contact networks where the cost of the relay contacts corresponding to x_i and $\bar{x}_i$ was the same. In networks consisting of electronic components, the cost of these two forms is different. It is certainly true that the cost of any network is independent of the labels on the inputs. For instance, the networks shown below cost the same in any type of technology.

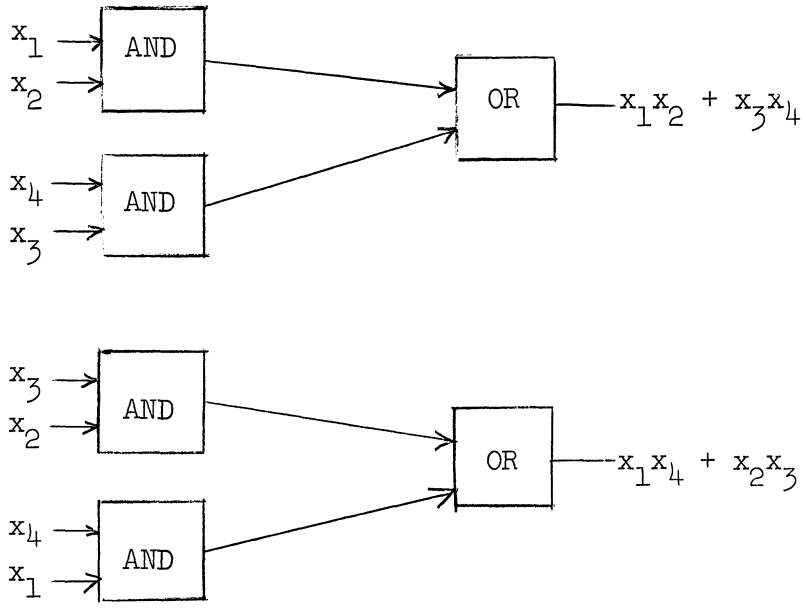

Fig. II. Two Networks Which Are Equivalent Under γ_3

$\mathcal{S}_n$ is used to denote the symmetric group on n letters; this group has order n! and degree n. $\mathcal{S}_n$ is now defined as an operator group on Boolean functions as suggested by the previous discussion.

Definition 1. For any $\sigma \in \mathcal{S}_n$ and any $f \in F_n$, define

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

The symmetric group on the variables has been studied by Hellerman[18] who was able to obtain the number of classes for $1 \leq n \leq 5$ by using Burnside's formula. Hellerman, however, did not have an algorithm for the solution of the general problem. This group has been mentioned implicitly in reference[9] but no explicit discussion is given. It is believed that the results which follow have not been obtained before.

Thus, every $\sigma \in \mathcal{S}_n$ induces a permutation of the atoms of F_n as shown in the following example where $\sigma = (12)$ and we consider F_3

$$\begin{aligned}
(0,0,0) &\longrightarrow (0,0,0)\\
(0,0,1) &\longrightarrow (0,0,1)\\
(0,1,0) &\longrightarrow (1,0,0)\\
(0,1,1) &\longrightarrow (1,0,1)\\
(1,0,0) &\longrightarrow (0,1,0)\\
(1,0,1) &\longrightarrow (0,1,1)\\
(1,1,0) &\longrightarrow (1,1,0)\\
(1,1,1) &\longrightarrow (1,1,1)
\end{aligned}$$

Using the conventional decimal notation for atoms (cf. [4]) and writing the permutation of the atoms induced by σ be written in cyclic notation, it is deduced that

$$\sigma \text{ induces } \quad h_\sigma = (0)(1)(6)(7)(2,4)(3,5)$$

Thus, the permutation σ of the variables induces a permutation h_σ of the domain.

Theorem 2. The mapping $\sigma \to h_\sigma$ for $\sigma \in \mathcal{S}_n$ is a one-to-one homomorphism from $\mathcal{S}_n$ into $\mathcal{S}_{2^n}$.

Proof. Clearly the mapping $\sigma \to h_\sigma$ is a map from $\mathcal{S}_n$ into $\mathcal{S}_{2^n}$. To show that the map is a homomorphism, suppose that

$$\sigma \to h_\sigma$$

$$\tau \to h_\tau$$

$$\sigma\tau \to h_{\sigma\tau}$$

Clearly $\quad h_{\sigma\tau} = h_\sigma h_\tau$

as may be seen from computing the effect of $h_{\sigma\tau}$ on any typical domain element. To show that the mapping is one-to-one, assume that

$$h_\sigma = h_\tau$$

for all domain elements, but this can only happen if $\sigma = \tau$. Thus, the connection between $\mathcal{S}_n$ on the variables and the symmetric group on the domain can be summed up by saying that there is an injection from $\mathcal{S}_n$ into $\mathcal{S}_{2^n}$. The cycle structure of $\mathcal{S}_n$ as a permutation group on n letters is known, but the present problem requires a representation of the group of degree 2^n.

Theorem 3. Permutations of the same cycle structure in $\mathcal{S}_n$ correspond to permutations of the same cycle structure under the injection.

Proof. Let h be the homomorphism from $\mathcal{S}_n$ into $\mathcal{S}_{2^n}$. Since all permutations of the same cycle structure are conjugates, it is sufficient to show that conjugates of σ in $\mathcal{S}_n$ correspond to conjugates of $h(\sigma)$ in $\mathcal{S}_{2^n}$. This is trivial since

$$h(\rho^{-1}\sigma\rho) = h(\rho^{-1})h(\sigma)h(\rho) = (h(\rho))^{-1}h(\sigma)h(\rho)$$

because h is a homomorphism.

An algorithm must be constructed to pass from the symmetric group on n letters to a representation of the group on 2^n letters. To accomplish this, the effect of a cycle of length k on the atoms of the Boolean algebra is calculated.

A cycle of length k only affects 2^k domain elements and furthermore, the non-zero elements of the domain can be considered to be in one-to-one correspondence with the integers modulo $(2^k - 1)$.

Lemma 4. *If q is any integer such that $0 \leq q \leq 2^k-1$, then the least positive d such that*

$$2^d q \equiv q \mod (2^k - 1)$$

must divide k. Conversely, every d which divides k must satisfy the congruence for some $0 \leq q \leq 2^k-1$.

Proof. First we will show the converse. If $d \mid k$, then

$$(2^d-1) \mid (2^k-1)$$

then $$2^k-1 = q(2^d-1)$$

or $$2^d q \equiv q \mod (2^k-1)$$

Thus, this argument tells us that for given d, the q to be chosen is the integer

$$q = \frac{2^k-1}{2^d-1}$$

To prove the first half, assume d is the least integer such that $2^d q \equiv q \bmod (2^k-1)$. Then since $2^k \equiv 1 \bmod (2^k-1)$

$$2^k q \equiv q \bmod (2^k-1)$$

Assume for the sake of contradiction that $k = dp + r$ where $0 \leq r < d$. Then

$$2^{dp}\, 2^r q \equiv q \mod (2^k - 1)$$

i.e.
$$q(2^d)^p\, q2^r \equiv q \mod (2^k - 1)$$

We shall use the fact that $2^d \equiv q \bmod (2^k-1)$ exactly p times until the previous congruence is reduced to

$$2^r q \equiv q \mod (2^k - 1)$$

This is a contradiction unless r=0, i.e. $d \mid k$.

Lemma 5. A cycle of length k in $\mathcal{S}_n$ induces permutations on the domain whose lengths are divisors of k and moreover every divisor of k is the length of some cycle.

Proof. Write the numbers from 0 to $2^k - 1$ in binary notation and in natural order. The effect of a permutation of length k can be obtained by removing the left-hand column and writing it as the right-hand column. This has the effect of doubling each number modulo $2^k - 1$. Thus a number q ($0 \leq q \leq 2^k - 1$) goes successively into $2q, 4q, \ldots, 2^d q \equiv q \bmod (2^k - 1)$. The length of the cycle containing q is the least positive integer d such that

$$2^d q \equiv q \bmod (2^k - 1)$$

By the use of lemma 4, the result is obtained.

Theorem 6. A cycle of length k in the symmetric group on the letters induces a permutation on the domain whose cycle structure is given by

$$\prod_{d|k} f_d^{e(d)}$$

where the f_d are the indeterminates of the cycle index and

$$e(m) = \frac{1}{m} \sum_{d|m} 2^d \mu\left(\frac{m}{d}\right)$$

where $\mu(\frac{m}{d})$ is the Möbius function.

Proof. Lemma 5 shows that the cycle lengths are exactly the divisors of k, but their multiplicity remains to be determined. Since the degree of the desired representation is 2^k, it is necessary that

$$\sum_{d|k} de(d) = 2^k$$

By the Möbius inversion formula,

$$e(k) = \frac{1}{k} \sum_{d|k} 2^d \mu(\frac{k}{d})$$

where $\mu(\frac{k}{d})$ is the Möbius function. It is interesting to note that e(k) is precisely the number of irreducible polynomials of degree k over GF(2).

Theorem 7. The cycle index for $\mathcal{S}_n$ as a permutation group on the domain of the Boolean algebra of functions is

$$Z_{\mathcal{S}_n} = \frac{1}{n!} \sum_{(j)} \frac{n!}{j_1!1^{j_1} j_2!2^{j_2} \ldots j_n!n^{j_n}} \bigtimes_{i=1}^{n} \left(\prod_{d|i} f_d^{e(d)} \right)^{\times j_i}$$

where the sum is over all partitions of n such that

$$\sum_{i=1}^{n} i j_i = n$$

and $\bigtimes_{i=1}^{n} y^{\times j_i} = y^{\times j_1} \times y^{\times j_2} \times \ldots \times y^{\times j_n}$ where $y^{\times j_i} = \overbrace{y \times y \times \ldots \times y}^{j_i}$.

Proof. The coefficient in the sum is the number of permutations of the n letters with j_i cycles of length i(i=1,...,n). To see this, choose any permutation with the required cycle structure. If all n! permutations are applied to the letters in the cycles, then the resulting permutations are not distinct for just two reasons, (1) the relative position of the cycles is irrelevant and (2) all cycles with the same elements in the same order are the same. The number of

duplications for the first reason is $j_1!\, j_2! \ldots j_n!$. The number of duplications for the second reason is $1^{j_1} 2^{j_2} \ldots n^{j_n}$ so that the desired number is

$$\frac{n!}{\prod_{i=1}^{n} j_i!\, i^{j_i}}$$

Turning now to the cycle structure, note that each cycle of length k affects 2^k elements of the domain and fixes all other domain elements. So the disjoint cycles act as if they were defined on disjoint sets. Cycles of length i go into cycles of length 2^i and finally that

$$\sum ij_i \rightarrow \prod 2^{ij_i} = 2^{\sum ij_i} = 2^n$$

This accounts for the presence of the cross operation even though the group structure is not that of a direct product.

Using this theorem, the cycle index has been constructed for γ_n for $1 \leq n \leq 6$ and these polynomials are to be found in appendix I.

Now replace each indeterminate in γ_n by two to obtain the total number of classes which are given below in Table III. T_n denotes the number of classes.

n	T_n
1	4
2	12
3	80
4	3,984
5	37,333,248
6	25,626,412,338,274,308

TABLE III

THE TOTAL NUMBER OF CLASSES UNDER $\mathcal{J}_n$

	n			N_n^k	
k	1	2	3	4	5
0	1	1	1	1	1
1	2	3	4	5	6
2	1	4	9	17	28
3		3	16	52	134
4		1	20	136	625
5			16	284	2,674
6			9	477	10,195
7			4	655	34,230
8			1	730	100,577
9				655	258,092
10				477	579,208
11				284	1,140,090
12				136	1,974,438
13				52	3,016,994
14				17	4,077,077
15				5	4,881,092
16				1	5,182,326
T_n	4	12	80	3,984	37,333,248

TABLE IV

THE NUMBER OF CLASSES OF FUNCTIONS WITH k ATOMS UNDER $\mathcal{J}_n$

Now we can apply Polya's theorem to count the number of classes of functions with k atoms in their normal form expansion. N_n^k denotes this number; we remark in passing that $N_n^k = N_n^{2^n-k}$. It is also true that $N_n^0 = 1$ and $N_n^1 = n + 1$ for all $n \geq 1$. Cf. Table IV.

Before concluding this description of the construction of cycle index of γ_n, an example is given. Let n=3 so that the partitions of 3 are

1) $j_1 = 3,\ j_2 = 0,\ j_3 = 0$

2) $j_1 = 1,\ j_2 = 1,\ j_3 = 0$

3) $j_1 = 0,\ j_2 = 0,\ j_3 = 1$

Thus

$$Z_{\gamma_3} = \frac{1}{6}\left((f_1^2)^{\times 3} + 3(f_1^2) \times (f_1^2 f_2) + 2f_1^2 f_3^2\right)$$

$$= \frac{1}{6}(f_1^8 + 3f_1^4 f_2^2 + 2f_1^2 f_3^2)$$

It is very interesting to note that one can carry the analysis one step further and write a completely closed form for Z_{γ_n}

Theorem 8.

$$Z_n = \frac{1}{n!} \sum_{(j)} \frac{n!}{\prod_{i=1}^{n} j_i! i^{j_i}} \prod_{i_1 | 1} \cdots \prod_{i_n | n} f^{(i_1,\ldots,i_n)}\, g_{j_1}(i_1) \cdots g_{j_n}(i_n)$$

$$< i_1,\ldots,i_n >$$

where

$$g_{j_k}(i_k) = \frac{1}{i_k} \sum_{d | i_k} 2^{d j_k} \mu\left(\frac{i_k}{d}\right) \qquad \text{for } k=1,\ldots,n$$

and the sum is over all partitions of n.

Proof. The result follows directly from theorem 7 and the properties of the cross operation.

3-6. $\mathcal{J}_n$, the Group of Complementations and Permutations of Variables

It seems very natural to consider the concept of equivalence when one can complement and permute variables. This situation was the first case considered in the development of combinatorial results on Boolean functions. The first systematic paper on this topic is by Pólya who quotes some partial results of Jevons and Clifford which date back to the nineteenth century.

In our discussion of this group, to be called $\mathcal{J}_n$, there are two alternative approaches. We can simply define $\mathcal{J}_n$ and note that Σ_2^n and γ_n are subgroups possessing certain structure. A preferable alternative is to try to construct $\mathcal{J}_n$ from Σ_2^n and γ_n. We choose this alternative because a similar process will be followed later on for two different groups.

First we shall consider symbols of the form (i,σ) where $i \in \Sigma_2^n$ and $\sigma \in \gamma_n$. We shall define such a symbol as operating on Boolean functions in the following way.

$$(i,\sigma)f(x_1,\ldots,x_n) = f(x_{\sigma(1)}^{i_1},\ldots,x_{\sigma(n)}^{i_n})$$

Clearly, the objects (i,σ) permute the domain as we would like, but our tacit comment that $\mathcal{J}_n$ is a group must be verified.

Theorem 1. $\mathcal{G}_n = \{(i,\sigma) \mid i \in \Sigma_2^n,\ \sigma \in \mathcal{S}_n\}$ is a group under the following operation

$$(i,\sigma)(j,\tau) = (i + \sigma(j),\ \sigma\tau)$$

where $\sigma(j)$ denotes

$$\sigma(j) = \sigma(j_1,\ldots,j_n) = (j_{\sigma(1)},\ldots,j_{\sigma(n)})$$

Proof. We first verify that the operation is associative.

$$((i,\sigma)\ (j,\tau))\ (k,\rho) = ((i + \sigma(j)),\ \sigma\tau)\ (k,\rho)$$

$$= (i + \sigma(j) + \sigma\tau(k),\ \sigma\tau\rho)$$

Now we compute

$$(i,\sigma)\ ((j,\tau)(k,\rho)) = (i,\sigma)\ (j + \tau(k),\ \tau\rho)$$

$$= (i + \sigma(j) + \sigma\tau(k),\ \sigma\tau\rho)$$

The rest of the verification of the group exioms is routine.

In the next two lemmas we note some facts about the abstract structure of the group.

Lemma 2.a. $(i,\sigma)^{-1} = (\sigma^{-1}(i),1)(0,\sigma^{-1})$

$$(\sigma(i),\sigma) = (0,\sigma)(i,1)$$

$$(0,\sigma)(i,\sigma^{-1}) = (\sigma(i),1)$$

Lemma 3. For $\sigma \in \mathcal{S}_n$ and $i \in \Sigma_2^n$ the application $\varphi_\sigma\colon i \to \sigma(i)$ is an automorphism of Σ_2^n.

Proof. Clearly φ_σ is a map from Σ_2^n into Σ_2^n. The map is onto since given any $j \in \Sigma_2^n$, then $\sigma^{-1}(j)$ maps onto j under φ_σ. The map is one-to-one since $\sigma(i) = \sigma(j)$ implies $i = \sigma^{-1}\sigma(i) = \sigma^{-1}\sigma(j) = j$. If $i \to \sigma(i)$, $j \to \sigma(j)$, and $i \oplus j \to \sigma(i \oplus j)$, then we have

$$\begin{aligned} \sigma(i \oplus j) &= \sigma(i_1 \oplus j_1, \ldots, i_n \oplus j_n) \\ &= (i_{\sigma(1)} \oplus j_{\sigma(1)}, \ldots, i_{\sigma(n)} \oplus j_{\sigma(n)}) \\ &= \sigma(i) + \sigma(j) \end{aligned}$$

and φ_σ is an automorphism.

In group theory, this process of combining Σ_2^n and γ_n to form $\mathcal{O}_n$ is a special case of forming the semi-direct product of Σ_2^n by γ_n. The following theorem is a special case of theorem 6.5.2 of Hall[14].

Theorem 4. *$\mathcal{O}_n$ is the semi-direct product of Σ_2^n by γ_n. The elements of the type $(0,\sigma)$ form a subgroup isomorphic to γ_n while the elements of the type $(i,1)$ form a normal subgroup isomorphic to Σ_2^n. Furthermore, $\Sigma_2^n \cap \gamma_n = (0,1)$ and $\Sigma_2^n \cup \gamma_n = \mathcal{O}_n$. The order of $\mathcal{O}_n$ is $n!2^n$.*

Proof. The result follows from Hall's definition and construction. All the stated properties are obvious except perhaps the normality of Σ_2^n. This follows directly from lemma 2, part c.

This result corrects an error of C. E. Shannon[37] who thought that the structure of $\mathcal{O}_n$ was the direct product of Σ_2^n and γ_n. This is obviously false since $((001),(123))((010),(132)) = ((001) \oplus (100), 1)) = ((101),1))$ when $((010),(132))((001),(123)) = ((010) \oplus (100), 1) = ((110), 1)$.

We may remark that this group operation of forming the semi-direct product is the abstract analog of the wreath product.

Before proceeding to the construction of $Z_{\mathcal{O}_n}$, certain interpretations of $\mathcal{O}_n$ should be pointed out. It is well known that the Boolean functions of n variables can be represented on the n-cube in the following way. Each of the 2^n-variables can be labeled with exactly one of the integers $0,1,\ldots,2^n-1$. If the label is written in its binary representation, there is a one-to-one correspondence between the domain elements of the Boolean functions and the vertices. Thus every subset of vertices corresponds to a Boolean function and conversely. The number of equivalence classes of Boolean functions under $\mathcal{O}_n$ is thus the same as the number of distinct ways that one can paint the vertices of the n-cube with two different colors. Two paintings of the n-cube are distinct, iff one can not be transformed into the other under the symmetry group of the cube. It is interesting to note that $\mathcal{O}_n$ is abstractly isomorphic to the hyper-octahedred group of Pólya, but not permutationally equivalent to it. The group must be isomorphic because the n-cube and the hyperoctahedron are dual figures and hence have isomorphic symmetry groups. The groups can be seen to be permutationally non-isomorphic since the degree of $\mathcal{O}_n$ is 2^n and the degree of the hyperoctahedred group is 2n.

Now the construction of $Z_{\mathcal{O}_n}$, is carried out. Certain facts will be used about the abstract structure of $\mathcal{O}_n$. The coefficients of $Z_{\mathcal{O}_n}$ will be just the coefficients of Z_{γ_n}. It is the cycle structure which changes. Every conjugate class in $\mathcal{O}_n$ has a cycle

in so-called normal form (cf. Ore, theorem 7). It is sufficient to consider a term of the form $((0,\ldots,0,1),(1,2,\ldots,k))$ by Ore's result. If the cycle structure induced by this term can be deduced, then we are done.

Lemma 5. The cycle lengths d induced by $((0,\ldots,0,1),(1,2,\ldots,k))$ have the property that $d \mid 2k$ but $d \nmid k$ and conversely.

Proof. The order of the permutation induced by $\alpha = ((0,\ldots,0,1),(1,\ldots,k))$ is 2k (theorem 4 of Ore). Thus, any cycle length d must divide 2k. If $d \mid k$, then $\alpha^k(q) = q$ for a domain element q in the cycle of length d. However, $\alpha^k = ((1,\ldots,1),1)$ which maps q into $2^n - 1 - q \neq q$. This contradiction shows that $d \nmid k$.

Conversely, suppose that $d \mid 2k$, but $d \nmid k$. We shall construct a formula for an integer q which lies in a cycle of length d; the formula will be given in terms of d and k. First, note that any d which divides 2k but does not divide k must be even. It is easily verified that a domain element of length k having the following form is invarient under α^d where $\alpha = ((0,\ldots,0,1),(1,2,\ldots,k))$.

$$\left(1^{\frac{d}{2}}, 0^{\frac{d}{2}}, 1^{\frac{d}{2}}, \ldots 0^{\frac{d}{2}}, 1^{\frac{d}{2}} \right)$$

The notation $1^{\frac{d}{2}}$ means $\overbrace{1, 1, \ldots, 1}^{d/2}$. The domain element will begin and end with $1^{\frac{d}{2}}$ because if the number of terms $\beta^{\frac{d}{2}}$ where $\beta \in \{0,1\}$ were even, say ℓ, then we would have $(\frac{d}{2})\ell = k$ or $(\frac{\ell}{2})d = k$ or that d would divide k, which would be a contradiction. To compute the

formula for this domain element we must simply compute the following sum

$$q = 1 + 2 + \ldots + 2^{\frac{d}{2}-1} + 2^{d} + \ldots + 2^{\frac{3d}{2}-1} + \ldots + 2^{k-\frac{d}{3}} + + \ldots + 2^{k-1}$$

$$= (2^{\frac{d}{2}} - 1) \sum_{i=0}^{\frac{2k-d}{2d}} 2^{id} = \frac{2^{\frac{2k+d}{2}} - 1}{2^{\frac{d}{2}} + 1}$$

For instance, if k=6, d=4, then q=51. It is easily checked that the cycle containing 51 is (12,25,38,51).

Lemma 6. The cycle structure induced by a cycle (1,...,k) is given by

$$\frac{1}{2}\left(\prod_{d|k} f_d^{e(d)} + \prod_{\substack{d|2k \\ d\nmid k}} f_d^{g(d)}\right)$$

where

$$e(k) = \frac{1}{k} \sum_{d|k} 2^{d}\, \mu(\tfrac{k}{d})$$

and

$$g(2k) = \frac{1}{2k} \sum_{\substack{d|2k \\ d\nmid k}} 2^{\frac{d}{2}}\, \mu(\tfrac{2k}{d})$$

where μ is the Möbius function.

Proof. A cycle of length k in the symmetric group induces a permutation of the type given in theorem 6, section 5 when premultiplied by a complementation having an even number of ones. The previous lemma computes the cycle lengths of the other case. We must require that

$$\sum_{\substack{d \mid 2k \\ d \nmid k}} dg(d) = 2^k$$

whence

$$g(2k) = \frac{1}{2k} \sum_{\substack{d \mid 2k \\ d \nmid k}} 2^{\frac{d}{2}} \mu\left(\frac{2k}{d}\right)$$

by a slight generalization of the Möbius inversion formula. To prove the generalization, it is sufficient to prove that

$$\sum_{\substack{d \mid 2k \\ d \nmid k}} \mu\left(\frac{2k}{d}\right) = \begin{cases} 1 & \text{if } k = 2p \\ 0 & \text{otherwise} \end{cases}$$

This is trivial since

$$\sum_{\substack{d \mid 2k \\ d \nmid k}} \mu\left(\frac{2k}{d}\right) = \sum_{\substack{t \mid k \\ t \text{ odd}}} \mu(t) = \sum_{\substack{t \mid \frac{k}{2^\alpha} \\ 2^\alpha \| k}} \mu(t) = \begin{cases} 1 & \text{if } k/2^\alpha = 1 \\ 0 & \text{otherwise} \end{cases}$$

Theorem 7. The cycle index of $\mathcal{O}_n$ is given by

$$Z_{\mathcal{O}_n} = \frac{1}{n!2^n} \sum_{(j)} \frac{n!2^n}{\prod_{i=1}^{n} j_i!(2i)^{j_i}} \prod_{i=1}^{n} \left(\prod_{d \mid i} f_d^{e(d)} + \prod_{\substack{d \mid 2i \\ d \nmid i}} f_d^{g(d)} \right)^{x_{j_i}}$$

where the sum is over all solutions of $\sum_{i=1}^{n} i j_i = n$.

Proof. The result follows directly from the lemmas by the same reasoning as in theorem 7, section 5.

As an example, $\mathcal{J}_2$ is computed

$$Z_{\mathcal{J}_2} = \frac{1}{8}\left((f_1^2 + f_2)^{\times 2} + 2(f_1^2 f_2 + f_4)\right) = \frac{1}{8}\left(f_1^4 + 3f_2^4 + 2f_1^2 f_2 + 2f_4\right)$$

$$Z_{\mathcal{J}_2}(1+x,\ 1+x^2,\ 1+x^3,\ 1+x^4) = 1 + x + 2x^2 + x^3 + x^4$$

The classes are shown below

$$[0]\ \left[\bar{x}\bar{y},\ \bar{x}y,\ x\bar{y},\ xy\right]\ \left[x,\ y,\ \bar{x},\ \bar{y}\right]$$

$$\left[x \oplus y,\ x \equiv y\right]\ \left[\bar{x}+\bar{y},\ \bar{x}+y,\ x+\bar{y},\ x+y\right]\ [1]$$

Table V indicates the number of classes for $1 \leq n \leq 1$ while Table VI shows the numbers N_n^k.

T_n	n
3	
6	
22	
402	
1,228,158	
400,507,806,843,728	

TABLE V

THE TOTAL NUMBER OF CLASSES UNDER $\mathcal{G}_n$

k \ n	1	2	3	4	5
			N_n^k		
0	1	1	1	1	1
1	1	1	1	1	1
2	1	2	3	4	5
3		1	3	6	10
4		1	6	19	47
5			3	27	131
6			3	50	472
7			1	56	1,326
8			1	74	3,779
9				56	9,013
10				50	19,963
11				27	38,073
12				19	65,664
13				6	98,804
14				4	133,576
15				1	158,658
16				1	169,112
T_n	3	6	22	402	1,228,158

TABLE VI

THE NUMBER OF CLASSES OF FUNCTIONS WITH k ATOMS UNDER $\mathcal{G}_n$

3-7. The Linear Group

Let $Z_2 = \{0,1\}$ be the field of two elements which must be of characteristic two. By $GL_n(Z_2)$, denote the group of all non-singular transformations from an n dimensional vector space over Z_2 into itself. Since the underlying field is finite, the order of $GL_n(Z_2)$ is also finite. It is well known (cf. Artin[1]) that the order of $GL_n(Z_2)$ is

$$\prod_{i=0}^{n-1} (2^n - 2^i) = 2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (2^i - 1)$$

For our purposes, it is convenient to think of $GL_n(Z_2)$ as a group of n x n non-singular matrices whose elements are zeroes and ones.

Let $A = (a_{ij})$ be such a matrix and let $f(x_1,\ldots,x_n) \in F_n$. We define the product Af as

$$Af(x_1,\ldots,x_n) = f\left(\sum_{k=1}^{n} \oplus a_{k1}x_k,\ldots,\sum_{k=1}^{n} \oplus a_{kn}x_k\right)$$

where $\oplus$ denotes addition modulo two. This may be abbreviated if $\underset{\sim}{x}$ denotes the row vector $(x_1,\ldots,x_n)$. Then we may write

$$Af(\underset{\sim}{x}) = f(\underset{\sim}{x}A)$$

The first problem to be posed is the determination of the number of classes, so we turn to the problem of finding $Z_{GL_n(Z_2)}$.

All of the available information necessary to calculate the cycle index is available in the literature. Dickson[8] (page 235) calculates the coefficients of the cycle index which are essentially the number of elements in a conjugacy class. Elspas[10] derives and Slepian[40]

uses the cycle structure for each class. Slepian[40] has solved related problems in counting the number of classes of codes under $GL_n(Z_2)$.

The algorithm to be presented involves a certain amount of notation. Consider the irreducible polynomials of $Z_2[x]$. For every positive integer m, there are at most a finite number of irreducible polynomials of degree m. Imagine the irreducible polynomials sorted by degree and enumerated. The polynomial $p(x) = x$ will be excluded from all our considerations. Let d_i denote the degree of the i^{th} irreducible polynomial and let e_i be the least integer such that polynomial $p_i(x)$ divides $x^{e_i} - 1$. Church[5] has listed irreducible polynomials for the first four prime moduli. Table VII indicates the first 22 polynomials along with values of d_i and e_i for Z_2.

Since the irreducible factors of $x^{2^n} - x$ are exactly the irreducible polynomials (mod 2) of all degrees which divide n, let I(m) be the number of irreducible polynomials in $Z_2[x]$ of degree m. By equating degrees we get

$$\sum_{m|n} m\, I(m) = 2^n$$

By the Möbius inversion formula, one gets

$$I(n) = \frac{1}{n} \sum_{d|n} 2^d \mu\left(\frac{n}{d}\right)$$

where $\mu(\frac{n}{d})$ is the Möbius function.

TABLE VII

TABLE OF IRREDUCIBLE POLYNOMIALS OVER Z_2

i	x^6	x^5	x^4	x^3	x^2	x	x^0	d_i	e_i
1						1	1	1	1
2					1	1	1	2	3
3				1	0	1	1	3	7
4				1	1	0	1	3	7
5			1	0	0	1	1	4	15
6			1	1	0	0	1	4	15
7			1	1	1	1	1	4	5
8		1	0	0	1	0	1	5	31
9		1	0	1	0	0	1	5	31
10		1	0	1	1	1	1	5	31
11		1	1	0	1	1	1	5	31
12		1	1	1	0	1	1	5	31
13		1	1	1	1	0	1	5	31
14	1	0	0	0	0	1	1	6	63
15	1	0	0	1	0	0	1	6	9
16	1	0	1	0	1	1	1	6	21
17	1	0	1	1	0	1	1	6	63
18	1	1	0	0	0	0	1	6	63
19	1	1	0	0	1	1	1	6	63
20	1	1	0	1	1	0	1	6	63
21	1	1	1	0	0	1	1	6	63
22	1	1	1	0	1	0	1	6	21

Because the polynomial $p(x) = x$ is ignored, we must subtract one from $I(n)$ in our calculations. Let t_n be the number of irreducible polynomials in $Z_2\ x$ of degree n or less not counting $p(x) = x$. Table VIII shows the first few values of $I(n)$ and t_n. Of course

$$t_n = \sum_{m=1}^{n} I(m) - 1$$

TABLE VIII

VALUES OF I_n AND t_n

n	I(n)	t_n
1	2	1
2	1	2
3	2	4
4	3	7
5	6	13
6	9	22

The first step in the algorithm is to give a notation for describing the classes of $GL_n(Z_2)$. One finds all possible non-negative integer solutions a_i of the equation

$$\sum_{i=1}^{t_n} a_i\, d_i = n$$

The solutions may be written as set of t_n-tuples $(a_1,\ldots,a_{t_n})$. Take every element a_i and write all possible partitions of a_i where the partitions must be written in the form

$$a_i = \sum_{j=1}^{a_i} j\alpha_{ij} \qquad (1)$$

Thus the α_{ij} are elements in the partition for the integer a_i. The classes of the group may be given by t_n-tuples each of whose elements is a partition of a solution of equation (1). The notation is just unusual enough that an example is in order.

Example: n=2. There are only 2 solutions of $a_1 + 2a_2 = 2$, namely $a_1 = 2$, $a_2 = 0$ and $a_1 = 0$, $a_2 = 1$. Thus there are 3 classes

$$(\alpha_{11} = 2, 0)$$

$$(\alpha_{12} = 1, 0)$$

$$(0, \alpha_{21} = 1)$$

Before writing down the cycle index, two final definitions are introduced. Let $q_{ij} = e_i 2^{b_j}$ where $b_j = -\left[-\log_2 j\right]$. $\left[x\right]$ is the largest integer $\leq x$. Also let

$$h_{ij} = \frac{2^{d_i(j-1)}\,(2^{d_i} - 1)}{q_{ij}}$$

At long last it is possible to write down a closed form for the cycle index.

Theorem 1. *The cycle index for $GL_n(Z_2)$ as a permutation group on the 2^n elements of $\{0,1\}^n$ is*

$$Z_{GL_n(Z_2)} = \frac{1}{2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (2^i-1)} \sum \frac{2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (2^i-1) \overset{t_n}{\underset{i=1}{\times}} \overset{a_i}{\underset{j=1}{\times}} \left(\prod_{k=1}^{j} f_1 f_{q_{ik}}^{h_{ik}} \right)^{\times \alpha_{ij}}}{\prod_{j=1}^{t_n} \left(\prod_{k=1}^{a_j} 2^{\alpha_{jk}^2 (k-1)} \prod_{k=1}^{a_j-1} \prod_{\ell=k+1}^{a_j} 2^{2k\alpha_{jk}\alpha_{j\ell}} \right)^{d_j} \prod_{p=1}^{a_j} 2^{d_j \frac{(\alpha_{jp}-1)\alpha_{jp}}{2}} \prod_{q=1}^{\alpha_{jp}} (2^{q\, d_j}-1)}$$

Proof. The complicated coefficient is merely the number of elements in the class as given by Dickson[8]. The products of f's denote the cycle structure as derived by Elspas[10].

Using the algorithm, the cycle index polynomials have been constructed for $1 \leq n \leq 6$. The number of classes is obtained by substituting 2 for each indeterminate. The results are given in Table IX. Further results are collected in Table X where N_n^k denotes this number while T_n denotes the total number of classes.

It is easily seen that $N_n^1 = 2$ for all n. This is because the zero vector is in a class by itself and all the other atoms are equivalent. If $n > 1$, then $N_n^2 = 2$. One class consists of the functions having the zero vector and another non-zero vector. The second class consists of functions involving two different non-zero vectors. The reason that any pair of such functions are equivalent is that there exists a nonsingular transformation which takes any basis onto any other basis. Likewise $n \geq 3$ implies $N_n^3 = 3$, and $n \geq 4$ implies $N_n^4 = 5$.

n	Number of Classes
1	4
2	8
3	20
4	92
5	2,744
6	950,998,216

TABLE IX

THE TOTAL NUMBER OF CLASSES UNDER $GL_n(Z_2)$

n	N_n^k				
k	1	2	3	4	5
0	1	1	1	1	1
1	2	2	2	2	2
2	1	2	2	2	2
3		2	3	3	3
4		1	4	5	5
5			3	7	8
6			2	9	14
7			2	11	23
8			1	12	35
9				11	55
10				9	84
11				7	117
12				5	158
13				3	204
14				2	242
15				2	274
16				1	290
T_n	4	8	20	92	2744

TABLE X

THE NUMBER OF CLASSES OF FUNCTIONS WITH k ATOMS UNDER $GL_n(Z_2)$

It is desirable to examine the structure of the equivalence classes themselves. The following considerations facilitate calculations. Every matrix in $GL_n(Z_2)$ may be written in row echelon form. This says that $GL_n(Z_2)$ is generated by the scalar matrices, the n! permutation matrices P_{ij} which interchange columns i and j, and the matrices D_{ij} which add the j^{th} column to the i^{th} column mod 2. An easy calculation shows that

$$P_{ij} = D_{ij} D_{ji} D_{ij}$$

Thus the group is generated by the $n^2 - n$ matrices D_{ij}. This means that to find functions equivalent to $f(x_1,\ldots,x_i,\ldots,x_n)$, one examines $f(x_1,\ldots,x_i \oplus x_j,\ldots,x_n)$ for $j \neq 1$.*

As an example, we list the eight classes for n=2.

$$[0]\ [1]\ [\bar{x}\bar{y}]\ [\bar{x}y,\ x\bar{y},\ xy]\ [x + y]$$

$$[\bar{x} + y,\ x + \bar{y},\ \bar{x} + \bar{y}]\ [x,\ y,\ x \oplus y]\ [\bar{x},\ \bar{y},\ x \equiv y]$$

3-8. The Affine Group

Let us consider now the affine group as a transformation group on Boolean functions. An affine transformation is of the form

$$y = \underset{\sim}{x}A \oplus \underset{\sim}{b}$$

where $A \epsilon GL_n(Z_2)$ and $\underset{\sim}{b}$ is a vector whose components $b_i \epsilon Z_2$ for i=1,...,n. $\oplus$ denotes componentwise addition modulo 2. We denote the affine group

---

*This argument also shows that the class L_n of all 2^{n+1} linear Boolean functions of n variables is mapped into itself under $GL_n(Z_2)$. There are four classes of linear functions under $GL_n(Z_2)$ for all n.

by $\mathcal{A}_n(Z_2)$. The effect of the affine group is the complementation of those variables of the Boolean function for which $b_i = 1$. The order of $\mathcal{GL}_n(Z_2)$ is

$$2^{\frac{n(n+1)}{2}} \prod_{i=1}^{n} (2^i - 1)$$

In an obvious way, the action of $\mathcal{A}_n(Z_2)$ decomposes the functions into equivalence classes. The problem of counting the number of classes has been solved by Nechiporuk [25] but his proof has not been published. The subgroup of the affine group consisting of translations only is the group Σ_2^n. This group of order 2^n is the group of all complementations of variables of Boolean functions. The algorithm to be derived makes use of the fact that the structure of $\mathcal{A}_n(Z_2)$ as a permutation group is $GL_n(Z_2) \otimes \Sigma_2$ where the operation is the product of permutation groups previously discussed in section 2.2.

We may note that one can form the semi-direct product of Σ_2^n and $GL_n(Z_2)$ in exactly the same way that was done for $\mathcal{J}_n$. In this case, the product operation is

$$(b_1, A_1)\ (b_2, A_2) = ((b_1 \oplus (b_2 A_1)),\ A_1 A_2)$$

Since forming $b_2 A_1$ effects an automorphism of Σ_2^n, the formation of the semi-direct product requires no additional verification.

As mentioned in chapter two, a general algorithm for the construction of $Z_{\mathcal{A} \otimes \mathcal{S}}$ is not yet known. The problem can be solved in the present case because we know $Z_{GL_n(Z_2)}$ and Z_{Σ_2} has only transpositions

as its non-identity cycle structure. If we let v_{ij} denote the cycle structure for a term in $Z_{GL_n(Z_2)}$, then we must inquire after the cycle structure of v_{ij} when pre-multiplied by (say) $(0,1)\ldots(2^n-2,\ 2^n-1)$.

These results have been worked out by Elspas[10] and are summarized below.

Lemma 2. The cycle structure of $\mathcal{M}_n(Z_2)$ is given by

$$u_{ij} = \begin{cases} 2^{j-1} \prod_{k=1}^{j} f_1 \, f_{q_{1k}}^{h_{1k}} + 2^{j-1} \, f_{q_{1j+1}}^{2^j/q_{1j+1}} \\ \\ 2^{ij} \prod_{k=1}^{j} f_1 \, f_{q_{ik}}^{h_{ik}} \qquad \text{if } i > 1 \end{cases}$$

Proof. Examine the v_{ij} pre-multiplied by the non-identity permutations of $\sum_2^n$.

Theorem 3. The cycle index for $\mathcal{M}_n(Z_2)$ is given by

$$Z_{\mathcal{M}_n(Z_2)} = \frac{1}{2^{\frac{n(n+1)}{2}} \prod_{i=1}^{n} (2^i-1)} \sum \frac{2^{\frac{n(n+1)}{2}} \prod_{i=1}^{n} (2^i-1)^{\bigtimes_{i=1}^{t_n} \bigtimes_{j=1}^{a_i} \alpha_{ij}}}{\prod_{j=1}^{t_n} \left(\prod_{k=1}^{a_j} 2^{\alpha_{jk}^2 (k+1)^{a_j-1}} \prod_{k=1}^{a_j} \prod_{\ell=k+1}^{a_j} 2^{2k\alpha_{jk}\alpha_{j\ell}} \right)^{d_j} \prod_{p=1}^{a_j} 2^{d_j \frac{(\alpha_{jp}-1)\alpha_{jp}}{2}} \prod_{q=1}^{\alpha_{jp}} (2^{qd_j}-1)}$$

where the sum is over all classes.

Using the polynomials constructed by this formula, the numerical results of Table XI were obtained. For $3 \leq n \leq 5$, the results agree with those of Nechiporuk[25]. Again N_n^k denotes the number of classes of functions with k atoms in their normal form expansion while T_n denotes the total number of classes.

The following results are suggested by Table XII.
$N_n^0 = N_n^1 = N_n^2 = 1$. If $n > 1$ then $N_n^3 = 1$, and if $n > 2$, then $N_n^4 = 2$. If $n > 3$, then $N_n^5 = 2$. The first equation is trivial to verify. Suppose $n \geq 3$ and consider the classes for k=3; any set of three vectors may be translated into a basis for a three dimensional space and hence all sets of triples are equivalent. The case k=3, n=2 is trivial since $N_2^3 = N_2^1 = 1$. Similar proofs may be furnished in the other cases. We note that the class L_n of linear Boolean functions is preserved under $\mathcal{A}_n(Z_2)$ and that there are 3 classes of linear functions for all n.

$$[\bar{x}\bar{y},\ \bar{x}y,\ x\bar{y},\ xy] \quad [\bar{x} + \bar{y},\ \bar{x} + y,\ x + \bar{y},\ x + y]$$

$$[x,\ \bar{x},\ y,\ \bar{y},\ x \oplus y,\ x \equiv y] \quad [0] \quad [1]$$

TABLE XI

THE TOTAL NUMBER OF CLASSES UNDER $\mathcal{M}_n(Z_2)$

n	T_n
1	3
2	5
3	10
4	32
5	382
6	15,768,919

TABLE XII

THE NUMBER OF CLASSES OF FUNCTIONS WITH k ATOMS UNDER $\mathcal{M}_n(Z_2)$

	N_n^k				
	1	2	3	4	5
0	1	1	1	1	1
1	1	1	1	1	1
2	1	1	1	1	1
3		1	1	1	1
4		1	2	2	2
5			1	2	2
6			1	3	4
7			1	3	5
8			1	4	8
9				3	9
10				3	15
11				2	16
12				2	23
13				1	24
14				1	30
15				1	30
16				1	38
T_n	3	5	10	32	382

3-9. Summary

In this chapter, we have defined five groups on switching functions and calculated their cycle indices using for the most part, structural properties of the permutation groups. The lattice structure of these subgroups is shown below in Figure III.

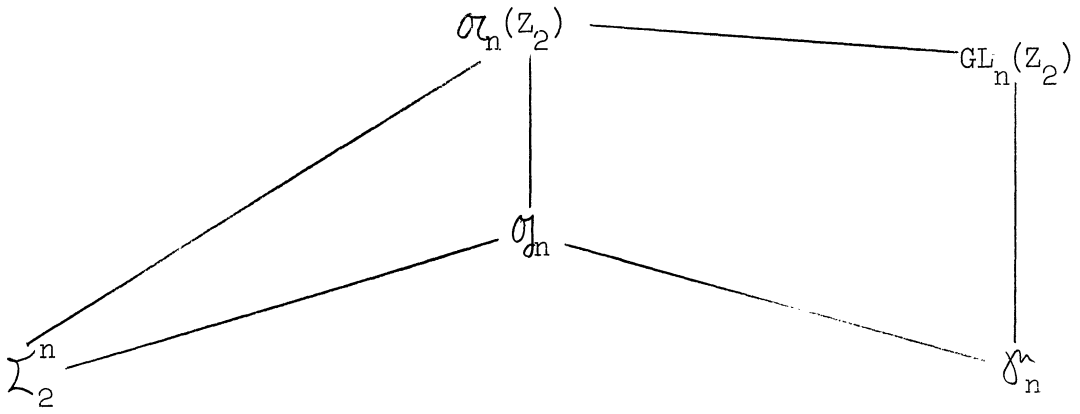

Fig. III. The Lattice of Interesting Subgroups of $\mathcal{A}_n(Z_2)$

For each of these groups, we have counted the number of classes. In the next chapter the definition of equivalence will be extended and some general theorems about enumerations of Boolean functions will be proven.

CHAPTER IV

EXTENSIONS OF EQUIVALENCE OF BOOLEAN FUNCTIONS

4-1. Introduction

In this chapter the results about the classification of Boolean functions will be extended in several directions. First, we shall allow operations on the domain and range simultaneously. Then networks of switching elements with different groups acting simultaneously on inputs and outputs will be considered. Finally networks composed entirely of one-to-one functions will be studied.

4-2. Negation on the Range

Let us extend the previous results about equivalence of functions by allowing negation of the functions also. It is convenient to obtain the negation of a Boolean function by the action of a negation group to be denoted by $\mathcal{N}$. $\mathcal{N}$ has order two; one element is the identity mapping and the other element, denoted by η, has the property:

$$\eta: f \longrightarrow \bar{f}$$

for any Boolean function f.

The situation is now as follows; we have a group $\mathcal{G}$ defined on the domain of the Boolean functions and a group $\mathcal{H}$ on the range. The pertinent group on the functions is the exponentiation group $\mathcal{H}^{\mathcal{G}}$. To count the number of such classes, we may apply the DeBruijn theorem once we have calculated $Z_{\mathcal{H}}$. The action of $\mathcal{H}$ on $\{0,1\}$ is to permute 0 and 1 so that $\mathcal{H}$ is actually the symmetric group of degree and order two.

Thus

$$Z_{\mathfrak{A}} = \frac{1}{2}(f_1^2 + f_2)$$

The following lemma facilitates the calculations in using DeBruijn's theorem.

Lemma 1. *A term* $h_1^{j_1} \dots h_r^{j_r}$ *in* $Z_{\mathfrak{H}}$ *gives rise to*

$$Z_{\mathfrak{H}}\left(\sum_{t|1} t j_t, \dots, \sum_{t|s} t j_t\right)$$

Proof. We compute $\frac{\partial}{\partial z_i}(h_1^{j_1} \dots h_r^{j_r})$.

This yields

$$\frac{\partial}{\partial z_i}(h_1^{j_1} \dots h_r^{j_r}) = \frac{\partial}{\partial z_i} \prod_{t=1}^{r} \exp\left(t j_t \sum_{k=1}^{\infty} z_{kt}\right)$$

$$= \frac{\partial}{\partial z_i} \exp\left(\sum_{t=1}^{r} \sum_{k=1}^{\infty} t j_t z_{kt}\right)$$

$$= \left(\exp \sum_{t=1}^{r} \sum_{k=1}^{\infty} t j_t z_{kt}\right) \sum_{t=1}^{r} \sum_{k=1} t j_t \delta_{i\,kt}$$

where $\delta_{i\,kt}$ is the Kronecker delta function, i.e.

$$\delta_{i\,kt} = \begin{cases} 1 & \text{if } i=kt \\ 0 & \text{otherwise} \end{cases}$$

Taking every z_i equal to zero gives

$$\frac{\partial}{\partial z_i}(h_1^{j_1} \cdots h_r^{j_r}) = \sum_{t|i} t_{j_t}$$

Theorem 2. Let $\mathcal{G}$ be any permutation group on the domain of Boolean functions. The number of classes of functions under $\mathcal{N}^{\mathcal{G}}$ (transformations of $\mathcal{G}$ on the domain and complementation of the range) is given by

$$\frac{1}{2}\left(Z_{\mathcal{G}}(2,2,\ldots,2) + Z_{\mathcal{G}}(0,2,0,2,\ldots,0,2)\right)$$

This theorem is applied to obtain the appropriate numbers for the five groups.

Theorem 3. The number of classes of functions with Γ_2^n on the domain and $\mathcal{N}$ on the range is

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

Proof. The result follows from the closed form for $Z_{\Gamma_2^n}$.

Theorem 4. The number of classes of functions with $\mathcal{S}_n$ on the domain and $\mathcal{N}$ on the range is exactly one half the number of classes with just $\mathcal{S}_n$ on the domain.

Proof. Since the domain elements corresponding to (0) and to (2^n-1) are symmetric, then every term of the cycle index contains a term f_1^k for $k \geq 2$.

Theorem 5. The number of classes of functions with $GL_n(Z_2)$ on the domain and $\mathfrak{N}$ on the range is exactly one half the number of classes with just $GL_n(Z_2)$ on the domain.

Proof. Every linear transformation leaves the origin invariant so every term of the cycle index contains a factor f_1^k for $k \geq 1$.

The calculated numerical results follow.

n	$\mathcal{L}_2^n$	$\mathcal{S}_n$	$\mathcal{G}_n$
1	2	2	2
2	5	6	4
3	30	40	14
4	2,288	1,992	222
5	67,172,352	18,666,624	616,126
6	144,115,192,303,714,304	12,813,206,169,137,152	200,253,952,527,184

n	$GL_n(Z_2)$	$\mathcal{A}_n(Z_2)$
1	2	2
2	4	3
3	10	6
4	46	18
5	1,372	206
6	475,499,108	7,888,299

TABLE XIII

NUMBER OF CLASSES UNDER GROUPS CONTAINING NEGATION

It is interesting to note the ease with which these results were obtained and to compare these methods with those of Elspas[11] and Ninomiya[26]. Both these men computed the same results but with considerable effort and only for the group $\mathcal{G}_n$.

4-3. Self-Complementary Classes

The results of the previous section are used to obtain some results concerning groups without negation on the range. Suppose $\mathcal{G}$ is a group on the domain and the number of classes of $\mathcal{G}$ closed under complementation of the functions is desired. Clearly only classes of neutral functions can have this property. Neutral functions are those functions with as many ones as zeroes in their graphs, i.e. functions of weight 2^{n-1}.

Theorem 1. The number of classes of functions under $\mathcal{G}$ which are equivalent to their complements, i.e. self-complementary, is

$$Z_{\mathcal{G}}(0,2,0,2,\ldots,0,2).$$

Proof. Let T_n be the number of classes of functions under $\mathcal{G}$ alone, note that $Z_G(2,\ldots,2) = T_n$. Let N_{sc} be the number of self-complementary classes. Then

$$\frac{1}{2}\left(Z_{\mathcal{G}}(2,\ldots,2) + Z_{\mathcal{G}}(0,2,\ldots,0,2)\right) = \frac{1}{2}\left(T_n - N_{sc}\right) + N_{sc}$$

which implies

$$N_{sc} = Z_{\mathcal{G}}(0,2,\ldots,0,2)$$

Theorem 2. The number of self-complementary classes under Γ_2^n is

$$(2^n - 1)\, 2^{2^{n-1}} - n$$

Proof. See the proof of theorem 3 in the previous section.

Theorem 3. There exists no self-complementary classes under γ_n.

Proof. See theorem 4, section 4-2.

Theorem 4. There exist no self-complementary classes under $GL_n(Z_2)$.

Proof. See theorem 5, section 4-2.

Now we show the results of the calculations.

n	Γ_n^2	γ_n	$\mathcal{A}_n$	$GL_n(Z_2)$	$\mathcal{A}_n(Z_2)$
1	1	0	1	0	1
2	3	0	2	0	1
3	14	0	6	0	2
4	240	0	42	0	4
5	63,488	0	4,094	0	30
6	4,227,858,432	0	98,210,640	0	7,679

TABLE XIV

NUMBER OF CLASSES OF SELF-COMPLEMENTARY FUNCTIONS

Elspas[11] made an interesting conjecture in relation to his solution of this problem. He suggested that the ratio of the number of self-complementary classes to the number of neutral classes went to zero for increasing n. This implies that the phenomenon of the self-complementary class is rather rare. Although Elspas made his conjecture for the group $\mathcal{A}_n$, we shall now derive it for $\mathcal{A}_n(Z_2)$. Then the result will be seen to hold for all groups whose orders satisfy an absolute inequality.

In order to obtain an answer we need a lower bound on the number of neutral classes and an upper bound on the number of self-complementary classes. These bounds are obtained in the following lemma.

Lemma 5. The number of neutral classes under $\mathcal{A}_n(Z_2)$ is greater than or equal to

$$\binom{2^n}{2^{n-1}} \frac{1}{2^{\frac{n(n+1)}{2}} \prod_{i=1}^{n} (2^i - 1)}$$

The number of self-complementary functions is less than or equal to

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

Proof. The first part is obtained by using the well known[22] lower bound $\frac{s}{g}$, where s is the number of objects on which a permutation group of order g acts. The result follows upon noting that there are $\binom{2^n}{2^{n-1}}$ neutral Boolean functions. The second part of the theorem follows from noting that the largest term in $Z_{\mathcal{A}}(0,2,\ldots,0,2)$ is $\frac{2^{2^{n-1}}}{g}$. An upper bound is certainly

$$\frac{1}{g} \sum_{\mathcal{A}} 2^{2^{n-1}} = 2^{2^{n-1}}$$

The desired ratio can now be computed, but it is convenient to have an estimate for the binomial coefficient. Using Stirling's formula, one can show that

$$\binom{2^n}{2^{n-1}} \sim \sqrt{\frac{2}{\pi}}\, 2^{2^n - \frac{n}{2}}$$

The ratio of self-complementary classes to neutral class under $\mathcal{A}_n(Z_2)$ is less than or equal to

$$\frac{2^{2^{n-1}}\, 2^{\frac{n(n+1)}{2}} \prod_{i=1}^{n} (2^i - 1)}{\binom{2^n}{2^{n-1}}} \sim \sqrt{\frac{\pi}{2}}\, \frac{2^{\frac{n(n+2)}{2}} \prod_{i=1}^{n} (2^i - 1)}{2^{2^{n-1}}} < \sqrt{\frac{\pi}{2}}\, \frac{2^{(n^2 + \frac{3}{2} n)}}{2^{2^{n-1}}} = o(1)$$

This shows that the ratio approaches zero for large n and therefore that self-complementary classes are rather rare. Thus, this result is also true for any group whose order is less than that of $\mathcal{A}_n(Z_2)$. One can show the following stronger result.

Theorem 6. *Let $\mathcal{G}$ be any group defined on the domain of F_n. If the order of $\mathcal{G}$ does not exceed*

$$\sqrt{\frac{2}{\pi}}\, 2^{2^{n-1} - \frac{n}{2} - \epsilon \log_2 n}$$

for any positive ϵ, then the number of self-complementary classes of functions tends to zero with the number of classes of neutral functions.

Proof. Compute the ratio for the upper bound.

4-4. Networks of Switching Functions

In this section, attention will be focused on networks of switching functions. The problem to be considered here is exactly the same as counting the number of classes of sequences of k Boolean functions of n variables. That is, the problem is that of classifying sequences of k Boolean functions of n variables under some transformation groups on n variables. One may think of the functions in these sequences as the transmission functions of a switching circuit having k outputs. See Fig. IV for a diagram of the generic network which will be called an (n,k) network. Our (n,k) networks realize the (k,n) sequences of Povarov[33].

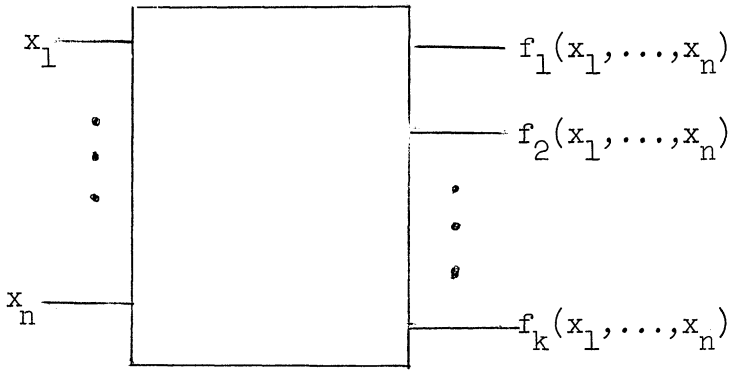

Fig. IV.

A Generic (n,k) Network

One may take either of two points of view in this investigation. Networks can be characterized by (1) their structure, i.e. the placement of certain components in arbitrary arrays or (2) by their behavior, i.e. the terminal relations. The former problem has been handled very neatly by Ninomiya[27] for the group of complementations and permutations.

Some related results of a special nature have been obtained by Sagalovitch[34] who obtained the number of one input k output networks whose transmission functions are non-trivial Boolean functions of n variables. In this discussion, the "behavioral" aspect of the problem is completely solved.

Before proceeding to the theoretical results, an example of two networks to be considered equivalent under $\mathcal{S}_3$ is given. Let $\sigma = (2,3) \in \mathcal{S}_3$ be applied to the inputs of the top network of Fig. V to give the bottom network of the figure.

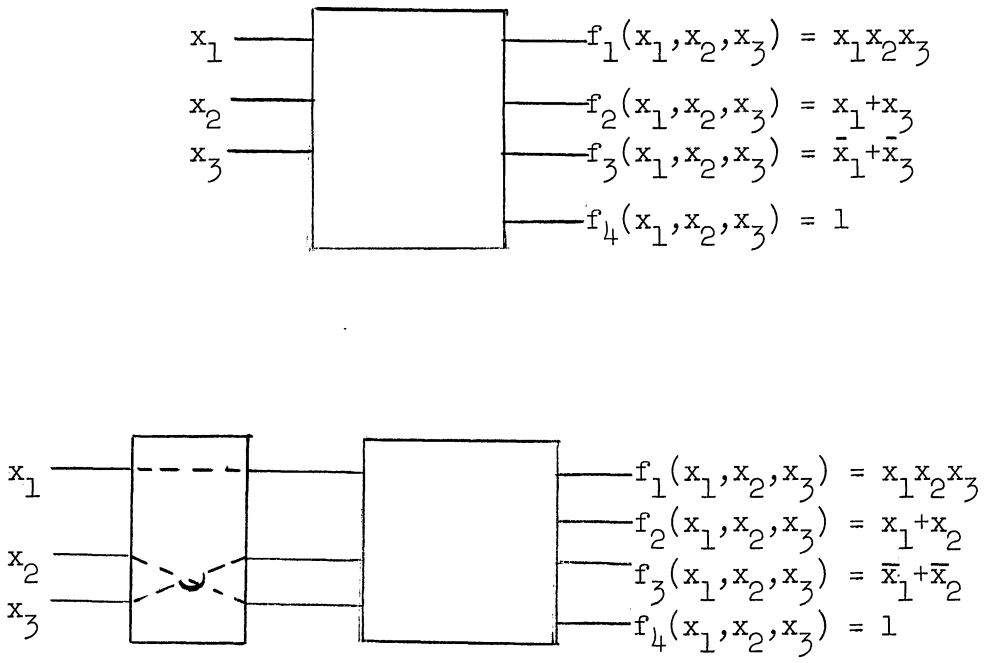

Fig. V.

The Effect of $\sigma = (2,3)$ on a (3,4) Network

The problem is now to count the number of classes of (n,k) networks under any group $\mathcal{G}$ acting on the domain of the functions, $\{0,1\}^n$. The total number of such networks is 2^{k2^n} since there are 2^{2^n} choices for each one of the k outputs.

In order to modify Pólya's formula for counting the number of classes of networks, note that no change has been made in the way that $\mathcal{J}$ acts on $\{0,1\}^n$. The only change is in the range. Mappings from $\{0,1\}^n$ into $\{0,1\}^k$ are now of interest so that a new figure counting series is needed. Obviously

$$\Psi(x_1,\ldots,x_{2^k}) = \sum_{i=1}^{2^k} x_i$$

Usually x_i is chosen to be one, but this is of no consequence.

Theorem 1. The number of equivalence classes of (n,k) networks (sequences of k Boolean functions of n variables) under a group $\mathcal{J}$ is given by

$$Z_{\mathcal{J}}(2^k,\ldots,2^k)$$

Proof. To count the total number of classes, one takes $x_i=1$ for $i=1,\ldots,2^k$ in the figure counting series. Thus f_i is replaced by

$$\sum_{j=1}^{2^k} 1^i = 2^k \qquad \text{for} \qquad i=1,\ldots,2^k$$

Corollary 2. The total number of classes of (n,k) networks under Γ_2^n is

$$\frac{1}{2^n}\left(2^{k2^n} + (2^n - 1)2^{k2^{n-1}}\right)$$

Proof. This follows from the fact that

$$Z_{\Upsilon_2^n} = \frac{1}{2^n}\left(f_1^{2^n} + (2^n - 1)f_2^{2^{n-1}}\right)$$

It is interesting to note that the class of all mappings from $\{0,1\}^n$ into $\{0,1\}^k$ forms a Boolean algebra of 2^{k2^n} functions in the natural way. It appears that the generalization of many problems in switching theory to the multiple output case can be handled naturally from this point of view.

The calculations have been carried out for the five groups under discussion and the results are given below in Tables XV through XIX. Certain facts may be deduced from the tables. For example, the number of classes under γ_1 and $GL_1(Z_2)$ is 4^k since these groups consist of the identity alone.

TABLE XV

THE NUMBER OF CLASSES OF NETWORKS UNDER Σ_2^n

n	k=1	k=2	k=3	k=4
1	3	10	36	136
2	7	76	1,072	16,576
3	46	8,416	2,100,736	536,928,256
4	4,336	268,496,896	17,592,201,773,056	1,152,921,508,633,378,816

TABLE XVI

THE NUMBER OF CLASSES OF NETWORKS UNDER μ_n

n	k=1	k=2	k=3	k=4
1	4	16	64	256
2	12	160	2,304	34,816
3	80	13,056	2,928,640	724,238,336
4	3,984	1,833,052,160	11,745,443,774,464	768,684,844,023,545,856

TABLE XVII

THE NUMBER OF CLASSES OF NETWORKS UNDER $\mathcal{G}_n$

n	k=1	k=2	k=3	k=4
1	3	10	36	136
2	6	55	666	9,316
3	22	1,996	384,112	91,604,416
4	402	11,756,666	735,192,450,952	48,047,227,408,513,056

TABLE XVIII

THE NUMBER OF CLASSES OF NETWORKS UNDER $GL_n(Z_2)$

n	k=1	k=2	k=3	k=4
1	4	16	64	256
2	8	80	960	13,056
3	20	1,056	135,040	27,700,736
4	92	320,416	14,333,211,520	916,495,047,958,016

TABLE XIX

THE NUMBER OF CLASSES OF NETWORKS UNDER $\mathcal{A}_n(Z_2)$

n	k=1	k=2	k=3	k=4
1	3	10	36	136
2	5	35	330	3,876
3	32	271	22,060	3,741,616
4	382	29,821	920,737,780	57,374,820,122,576

While the results of the previous paragraph are of some interest, certain networks are considered non-equivalent which differ only in the order of the outputs. It is desirable to enlarge our definition of equivalence of networks by allowing permutations in the range. More precisely, let the symmetric group on k letters, $\mathcal{S}_k$, act on the range, and consider two networks equivalent if and only if there is an $\alpha \in \mathcal{A}$ and a permutation $\sigma \in \mathcal{S}_k$ such that $(f_1(d),\ldots,f_k(d))$ $= (g_{\sigma(1)}(\alpha d),\ldots,g_{\sigma(k)}(\alpha d))$ for every $d \in \{0,1\}^n$. This instance is a special case of the DeBruijn theorem. The calculations have been carried out and are given in Tables XX through XXIV. The number of classes with (say) Σ_2^n on the domain and $\mathcal{S}_k$ on the range is denoted by $T(\Sigma_2^n, \mathcal{S}_k)$.

TABLE XX

THE NUMBER OF CLASSES OF NETWORKS WITH Γ_2^n ON THE INPUTS AND μ_k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	3	7	13	22
2	7	46	237	1,056
3	46	4,336	356,026	22,921,696
4	4,336	134,281,216	2,932,175,712,336	48,042,795,872,587,776

TABLE XXI

THE NUMBER OF NETWORKS WITH μ_n ON THE INPUTS AND μ_k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	4	10	20	35
2	12	88	484	2,180
3	80	6,616	497,760	31,017,356
4	3,984	916,539,904	1,957,701,217,238	32,031,538,353,966,080

TABLE XXII

THE NUMBER OF NETWORKS WITH α_n ON THE INPUTS AND μ_k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	3	7	13	22
2	6	34	158	652
3	22	1,056	66,336	3,945,992
4	402	5,884,954	122,543,247,874	2,002,161,498,159,934

TABLE XXIII

THE NUMBER OF NETWORKS WITH $GL_n(Z_2)$ ON THE INPUTS AND μ_k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	4	10	20	35
2	8	46	220	897
3	20	556	23,932	1,214,454
4	92	160,932	2,390,063,996	38,192,408,400,654

TABLE XXIV

THE NUMBER OF NETWORKS WITH $\mathcal{O}_n(Z_2)$ ON THE INPUTS AND $\mathcal{J}_k$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	3	7	13	22
2	5	22	87	314
3	10	153	4,148	169,495
4	32	15,209	153,668,757	2,391,065,770,697

If complementation of the k outputs of the networks is allowed, then two networks are equivalent if there is an $\alpha \in \mathcal{O}$ and an $i = (i_1,\ldots,i_k) \in \sum_2^k$, such that $(f_1(d),\ldots,f_k(d)) = (f_1^{i_1}(\alpha(d)),\ldots,f_k^{i_k}(\alpha(d))$ for all $d \in \{0,1\}^n$. The notation $f_j^{i_j}(d)$ is defined as

$$f_j^{i_j}(d) = \begin{cases} f_j(d) & \text{if } i_j = 0 \\ \bar{f}_j(d) & \text{if } i_j = 1 \end{cases} \qquad \text{for } j=1,\ldots,k$$

The number of such classes can again be determined from DeBruijn's theorem.

Theorem 3. The number of classes of (n,k) networks with a group $\mathcal{G}$ on the domain and the complementing group Σ_2^k on the range is

$$\frac{1}{2^k}\left(Z_{\mathcal{G}}(2^k,\ldots,2^k) + (2^k - 1)Z_{\mathcal{G}}(0,2^k,\ldots,0,2^k)\right)$$

The closed form of theorem 3 arises from the closed form $Z_{\Sigma_2^n}$. Note that the case when k=1 is exactly the case considered in section 4-2. The calculations are shown below in Tables XXV through XXIX.

TABLE XXV

THE NUMBER OF NETWORKS WITH Σ_2^n ON THE INPUTS AND Σ_2^k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	4	8	16
2	5	22	176	1,216
3	30	2,128	265,728	33,611,776
4	2,288	67,127,296	2,199,025,221,832	72,057,598,064,459,776

TABLE XXVI

THE NUMBER OF NETWORKS WITH $\mathcal{U}_n$ ON THE INPUTS AND Σ_2^k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	4	8	16
2	6	40	288	2,176
3	40	3,264	366,080	45,264,896
4	1,992	458,263,040	1,468,180,471,808	48,042,802,751,471,616

TABLE XXVII

THE NUMBER OF NETWORKS WITH $\mathcal{A}_n$ ON THE INPUTS AND Γ_2^k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	4	8	16
2	4	19	106	676
3	14	556	49,008	5,742,016
4	222	2,945,738	91,901,007,752	2,877,952,247,834,656

TABLE XXVIII

THE NUMBER OF NETWORKS WITH $GL_n(Z_2)$ ON THE INPUTS AND Γ_2^k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	4	8	16
2	4	20	120	816
3	10	264	16,880	1,731,296
4	46	80,104	1,791,651,440	51,030,940,434,876

TABLE XXIX

THE NUMBER OF NETWORKS WITH $\mathcal{A}_n(Z_2)$ ON THE INPUTS AND Σ_2^k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	4	8	16
2	3	11	50	276
3	6	79	2,908	236,176
4	18	7,621	115,125,476	3,585,934,560,176

It is somewhat artificial to consider complementation of the outputs only. One would prefer to consider both symmetries and complementations on the range. This suggests considering the least group containing $\mathcal{S}_k$ and Σ_2^k, i.e. we shall define $\mathcal{G}_k$ on the range. Without more ado, the calculations are presented in Tables XXX-XXXIV.

TABLE XXX

THE NUMBER OF NETWORKS WITH Σ_2^n ON THE INPUTS AND α_n ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	3	4	5
2	5	18	51	122
3	30	1,200	45,777	1,476,032
4	2,288	33,601,536	366,543,984,720	3,002,400,587,673,600

TABLE XXXI

THE NUMBER OF NETWORKS WITH μ_n ON THE INPUTS AND α_k ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	3	4	5
2	6	24	98	194
3	40	1,676	63,440	1,992,430
4	1,992	235,384,592	244,644,311,176	2,002,158,848,764,301

TABLE XXXII

THE NUMBER OF NETWORKS WITH $\mathcal{G}_n$ ON THE INPUTS AND $\mathcal{G}_k$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	3	4	5
2	4	13	34	640
3	14	308	8,906	257,658
4	222	1,476,218	15,320,103,918	125,147,156,711,032

TABLE XXXIII

THE NUMBER OF NETWORKS WITH $GL_n(Z_2)$ ON THE INPUTS AND $\mathcal{G}_k$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	3	4	5
2	4	13	36	95
3	10	146	3,178	80,036
4	46	40,422	298,842,656	2,387,346,322,704

TABLE XXXIV

THE NUMBER OF NETWORKS WITH $\mathcal{G}_n(Z_2)$ ON THE INPUTS AND $\mathcal{G}_k$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	3	4	5
2	3	8	19	41
3	6	49	632	11,917
4	18	3,963	19,245,637	149,471,180,139

DeBruijn's theorem allows us to consider any group $\mathcal{G}$ on the domain and any group $\mathcal{H}$ on the range. The analysis of all remaining cases is completed by allowing $GL_n(Z_2)$ and $\mathcal{A}_n(Z_2)$ on the range. The results are given in Tables XXXV through XLIV.

TABLE XXXV

THE NUMBER OF NETWORKS WITH $\mathcal{L}_2^n$ ON THE INPUTS AND $GL_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	3	4	4	4
2	7	21	27	28
3	46	1,531	14,056	39,839
4	4,336	44,782,251	104,751,025,086	57,280,291,273,345

TABLE XXXVI

THE NUMBER OF NETWORKS WITH $\mathcal{U}_n$ ON THE INPUTS AND $GL_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	4	5	5	5
2	12	35	46	47
3	80	2,266	19,930	55,767
4	3,984	305,552,546	69,945,183,326	38,191,772,055,973

TABLE XXXVII

THE NUMBER OF NETWORKS WITH $\mathcal{G}_n$ ON THE INPUTS AND $GL_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	3	4	4	4
2	6	16	21	22
3	22	392	2,920	7,923
4	402	1,966,074	4,379,140,552	2,387,316,975,717

TABLE XXXVIII

THE NUMBER OF NETWORKS WITH $GL_n(Z_2)$ ON THE INPUTS AND $GL_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	4	5	5	5
2	8	20	27	28
3	20	206	1,204	3,071
4	92	54,155	85,552,416	45,568,388,658

TABLE XXXIX

THE NUMBER OF NETWORKS WITH $\mathcal{A}_n(Z_2)$ ON THE INPUTS AND $GL_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	3	4	4	4
2	5	11	15	16
3	10	64	276	653
4	32	5,276	5,534,421	178,471,391

TABLE XL

THE NUMBER OF NETWORKS WITH Σ_2^n ON THE INPUTS AND $\mathcal{A}_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	2	2	2
2	5	9	10	10
3	30	443	2,104	3,763
4	2,288	11,211,435	13,098,898,366	3,585,768,962,689

TABLE XLI

THE NUMBER OF NETWORKS WITH μ_n ON THE INPUTS AND $\Pi_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	2	2	2
2	6	11	12	12
3	40	590	2,828	5,066
4	1,992	76,384,114	8,747,130,342	2,390,901,609,645

TABLE XLII

THE NUMBER OF NETWORKS WITH α_n ON THE INPUTS AND $\Omega_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	2	2	2
2	4	7	8	8
3	14	124	504	880
4	222	494,298	547,849,868	539,100,216

TABLE XLIII

THE NUMBER OF NETWORKS WITH $GL_n(Z_2)$ ON THE INPUTS AND $\mathcal{A}_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	2	2	2
2	4	7	8	8
3	10	60	214	368
4	46	13,733	10,724,116	2,854,852,383

TABLE XLIV

THE NUMBER OF NETWORKS WITH $\mathcal{N}_n(Z_2)$ ON THE INPUTS AND $\mathcal{N}_k(Z_2)$ ON THE OUTPUTS

n	k=1	k=2	k=3	k=4
1	2	2	2	2
2	3	5	6	6
3	6	24	70	116
4	18	1,430	700,173	179,125,249

4-5. Invertible Boolean Functions

There is another interesting question to ask about the (n,k) networks. This problem is to determine the number of classes of invertible functions on networks. C. S. Lorens has studied this problem, and his results will be derived and generalized [22].

Since Boolean functions are also ordinary functions, a function f is invertible (i.e. has an inverse) if and only if f is one-to-one and onto. That is, consider the one-to-one onto mappings of $\{0,1\}^n$ into $\{0,1\}^n$. These are just the $2^n!$ permutations of $\{0,1\}^n$.

Theorem 10 of section 2-1 was proved in this thesis for this application. We shall now derive a lemma which will facilitate the calculations.

Lemma 1. A term of the form

$$\left[a \frac{\partial^{m_1}}{\partial z_{i_1}} \frac{\partial^{m_2}}{\partial z_{i_2}} \cdots \frac{\partial^{m_s}}{\partial z_{i_s}} \; b(1+k_1 z_{k_1})^{j_1} \cdots (1+k_s z_{k_s})^{j_s} \right]_{z_1 = z_2 = \cdots = z_s = 0}$$

yields

$$\begin{cases} ab \prod_{p=1}^{s} k_p^{m_p} m_p! & \text{if } i_1 = k_1, \ldots, i_s = k_s \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Notice that unless the cycle structure of the term involving the differential operator is the same as the term involving the variables, the result will be zero. If $i_1 = k_1, \ldots, i_s = k_s$, then $m_1 = j_1, \ldots, m_s = j_s$ and the result follows from the rules of differentiation.

First apply this lemma to the case where $\sum_2^n$ acts on both the domain and the range.

Theorem 2. The number of classes with $\sum_2^n$ acting on both the range and the domain is given by

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

Before proceeding to the calculations, the reader is reminded of a remark made in the proof of theorem 2-1-10. We noted at that time that the mapping $f \to f^{-1}$ is one-to-one. From this fact, it was remarked that the number of classes with a group $\mathcal{O}_f$ on the domain and a group $\mathcal{H}_g$ on the range is the same as the number of classes when $\mathcal{H}_g$ acts on the domain and $\mathcal{O}_f$ on the range. The calculations for the other cases have been carried out and are summarized in Tables XLVI and XLVII. Table XLV shows the number of invertible functions. It would require a computer to evaluate the results for n=5 and most computers would require at least triple precision arithmetic to accomplish this.

TABLE XLV

THE NUMBER OF INVERTIBLE FUNCTIONS

n	
1	2
2	24
3	40,320
4	20,922,789,888,000

TABLE XLVI

THE NUMBER OF CLASSES OF INVERTIBLE FUNCTIONS WITH THE SAME GROUP ON BOTH THE DOMAIN AND THE RANGE

n	Σ_2^n	$\mathcal{M}_n$	$\mathcal{N}_n$	$GL_n(Z_2)$	$\mathcal{O}\ell_n(Z_2)$
1	1	2	1	2	1
2	6	7	2	2	1
3	924	1,172	52	10	4
4	81,738,720,000	36,325,278,240	142,090,700	52,246	302

TABLE XLVII

THE NUMBER OF CLASSES OF INVERTIBLE FUNCTIONS
WITH DIFFERENT GROUPS ON THE DOMAIN AND RANGE

n	Γ_2^n on Domain $\mathcal{U}_n$ on Range	Γ_2^n on Domain $\mathcal{A}_n$ on Range	$\mathcal{U}_n$ on Domain $\mathcal{A}_n$ on Range
1	1	1	1
2	3	3	2
3	840	196	154
4	54,486,432,000	3,406,687,200	2,270,394,624

n	Γ_2^n on domain $GL_n(Z_2)$ on range	$\mathcal{U}_n$ on domain $GL_n(Z_2)$ on range	$\mathcal{A}_n$ on domain $GL_n(Z_2)$ on range
1	1	2	1
2	1	3	1
3	30	56	10
4	64,864,800	43,265,728	2,705,820

n	Γ_2^n on domain $\mathcal{O}_n(Z_2)$ on range	$\mathcal{U}_n$ on domain $\mathcal{O}_n(Z_2)$ on range	$\mathcal{G}_n$ on domain $\mathcal{O}_n(Z_2)$ on range	$GL_n(Z_2)$ on domain $\mathcal{N}_n(Z_2)$ on range
1	1	1	1	1
2	1	1	1	1
3	16	10	8	4
4	4,073,400	2,705,820	172,194	3374

One might be interested in comparing the results of the previous section with these results on invertible functions. In both cases n-input, n-output networks with groups on the domain and the range were studied but now the functions are required to have inverses. Comparing the results of this section against $T(\mathcal{O}_J, \mathcal{h}_J)$ for (n,n) networks, one finds that the ratio of the number of classes of invertible functions to $T(\mathcal{O}_J, \mathcal{h}_J)$ approaches zero for large n. Thus, the invertible classes are comparatively rare.

CHAPTER V

APPLICATIONS

5-1. Switching Theory

Chapter I presents a brief history of the development of combinatorial methods in switching theory. In this section, the principal applications of $\mathcal{J}_n$ to synthesis problems in the theory of switching are presented.

Since we shall have occasion to discuss the group invariance problem for switching functions in some detail, the problem is stated precisely. The problem is to find a complete set of invariants $\epsilon_1,\ldots,\epsilon_k$ of a group $\mathcal{J}$ defined on switching functions such that for any two functions f and g, f and g are equivalent iff

$$\epsilon_i(f) = \epsilon_i(g) \qquad \text{for } i=1,\ldots,k$$

The background for the use of $\mathcal{J}_n$ in synthesizing switching functions of four variables is as follows. Pólya[31] first showed that the 65,536 Boolean functions of four variables are resolved into 402 symmetry classes by $\mathcal{J}_n$. The Harvard Computation Laboratory[17] computed a representative function from each class. Golomb[12] found a complete set of invariants for $\mathcal{J}_n$ and gave a canonical form for switching functions.

In unpublished works, Moore, Gould, and others have compiled absolutely minimal networks for the 402 representative functions of four variables. An early version of the table is reprinted in Higgonet and Grea[19].

Example: Given the function $f(x_1,x_2,x_3)) = \bar{x}_1\bar{x}_2\bar{x}_3 + x_1\bar{x}_2x_3 + x_1x_2x_3$, construct a minimal network for realizing f. f can be seen to be equivalent to the function

$$x_2x_3 + x_1\bar{x}_2\bar{x}_3$$

under the transformation ((010), (12)(3)). The latter function is known to have the absolutely minimal network shown in Fig. VI. (See Seshu and Reed[35].

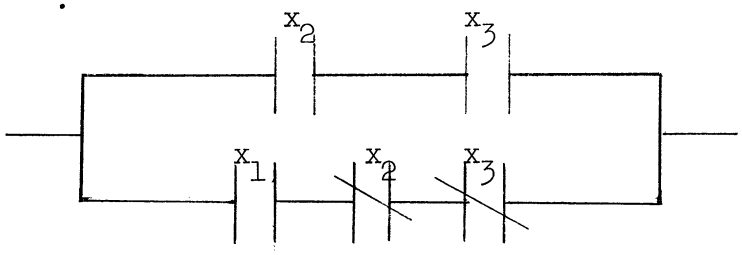

Fig. VI.

The Absolutely Minimal Network for $x_1\bar{x}_2\bar{x}_3 + x_2x_3$

It would seem desirable to extend this general procedure for the group $\mathcal{O}_n(Z_2)$. This group is so large that the enumeration of classes could be carried out for n=5 if we could solve the group invariance problem for $\mathcal{O}_n(Z_2)$. All the practical applications of our ideas to switching theory require the solution of this problem, and it is strictly a non-trivial problem.

At the present time, the group invariance problem has been solved for $\mathcal{O}_n$ by Golomb. Since the solution of the problem for the unimodular group in a related case is given by Weyl[42], and because the unimodular group is identical to $GL_n(Z_2)$ over the field of two elements, a partial solution to the invariance problem for $GL_n(Z_2)$ is known.

The finding of solutions for these group invariance problems is a

difficult, but an important task. The extension of this synthesis approach sketched above is important in switching theory. The solution of the invariance problem would also provide a canonical form for codes, but this latter problem will be considered next.

5-2. Error Correcting Codes

A problem of considerable importance in the theory of error correcting codes is the problem of enumerating equivalent codes. Slepian[41] has solved this problem for (n,k) codes under the general linear group. In this section, the connection between our results and those of Slepian will be indicated. In particular, Slepian's work is extended by giving the number of (n,k) codes under $\mathcal{H}_k(Z_2)$. For the purposes of the development, it is assumed that the reader is familiar with the theory of group codes which was developed, to a large extent, by Slepian; this material is reported in an easily readable form in reference[29]. The notation used in this section is compatible with the literature of coding theory, but unfortunately, differs somewhat from the rest of the thesis.

Consider the vector space of n-tuples over Z_2; a sub-space of dimension k is called an (n,k) code. Such a code contains 2^k vectors. A more compact description is obtained by considering the code to be given as the basis of the subspace. If the basis vectors are written in a k x n matrix G, then G is called the generator matrix of the (n,k) code and G is of rank k. Two generator matrices of (n,k) codes Ω_1 and Ω_2, are said to be equivalent iff there exists an $A \epsilon GL_k(Z_2)$ and there is an n x n permutation matrix P such that $\Omega_1 = A \Omega_2 P$.

The quantities which are desired are the following:

T_{nk}: The number of equivalence classes of k x n matrices with no columns of zeroes.

$\bar{T}_{nk}$: The number of equivalence classes of k x n matrices with no repeated rows and no columns of zeroes.

S_{nk}: The number of equivalence classes of (n,k) codes with no columns of zeroes.

$\bar{S}_{nk}$: The number of equivalence classes of (n,k) codes with no repeated columns and no columns of zeroes.

W_{nk}: The number of equivalence classes of (n,k) codes allowing zero columns and repetitions.

N_{nk}: The total number of distinct (n,k) codes.

First, Slepian's results for $GL_k(Z_2)$ are derived and then extended to $\mathcal{O}l_k(Z_2)$. In his first paper, Slepian showed that

$$N_{nk} = \frac{\prod_{i=0}^{k-1} (2^n - 2^i)}{\prod_{i=0}^{k-1} (2^k - 2^i)} .$$

A simple calculation shows that

$$W_{nk} = \sum_{i=1}^{n} S_{ik}$$

and also that the S's are related to the T's by

$$S_{nk} = T_{nk} - T_{n,k-1}$$

$$\bar{S}_{nk} = \bar{T}_{nk} - \bar{T}_{n,k-1}.$$

Thus, all the problems can be solved by computing T_{nk} and $\bar{T}_{n,k}$.

Theorem 1. $T_{n,k}$ *is given as the coefficient of* x^n *in*

$$Y_{GL_k(Z_2)}\ (1+x,\ 1+x^2,\ldots,1+x^{2^n})$$

where

$$Y_{GL_k(Z_2)}\ (f_1,\ldots,f_{2^n}) = \frac{1}{f_1}\ Z_{GL_k(Z_2)}\ (f_1,\ldots,f_{2^n}).$$

Proof. The transition from switching functions having n minterms and k variables to a k x n matrix occurs by writing the minterms as row vectors of a n x k matrix and transposing the matrix. Exclusion of the zero-columns of a matrix is the same as excluding the minterm $\bar{x}_1 \ldots \bar{x}_n$. This is accomplished by dividing out by f_1 in the cycle index of $GL_k(Z_2)$.

Theorem 2. T_{nk} *is given as the coefficient of* x^n *in*

$$Y_{GL_k(Z_2)}\ \left(\frac{1}{1-x},\ldots,\frac{1}{1-x^{2^n}}\right)$$

Proof. The store enumerating series is

$$1 + x + x^2 + \ldots = \frac{1}{1-x}$$

Note that this is the first time that we have had to endure an infinite series for the store generating function.

Sample Calculation: Suppose k=2. Then from appendix III,

$$Z_{GL_2(Z_2)} = \frac{1}{6}(f_1^4 + 3f_1^2f_2 + 2f_1f_3)$$

$$Y_{GL_2(Z_2)} = \frac{1}{6}(f_1^3 + 3f_1f_2 + 2f_3)$$

$$Y_{GL_2(Z_2)}(1+x, 1+x^2, 1+x^3) = 1 + x + x^2 + x^3$$

Thus

$$T_{i2} = 1 \quad \text{for } i=0,\ldots,3$$

$$T_{i2} = 0 \quad \text{for } i \geq 4$$

$$Y\left(\frac{1}{1-x}, \frac{1}{1-x^2}, \frac{1}{1-x^3}\right) = \frac{1}{6}\left(\sum_{j=0}^{\infty}\binom{j+2}{2}x^j + 3\sum_{j=0}^{\infty}\left[\frac{j}{2}+1\right]x^j + 2\sum_{j=0}^{\infty}x^{3j}\right)$$

The coefficient of x^n is

$$\frac{n^2+6n+12}{12} \quad \text{if } n \equiv 0 \bmod 6$$

$$\frac{(n+5)(n+1)}{12} \quad \text{if } n \equiv 1, 5 \bmod 6$$

$$\frac{(n+4)(n+2)}{12} \quad \text{if } n \equiv 2, 4 \bmod 6$$

$$\frac{(n+3)^2}{12} \quad \text{if } n \equiv 3 \bmod 6$$

Now the case of the affine group is considered. Equivalence under $\mathcal{A}_k(Z_2)$ is also a natural concept. Since the columns of zero no longer play a special role, then one need only compute the following quantities,

T_{nk} and $\bar{T}_{nk}$ where we now use these symbols in their previous meanings except for dropping the condition on zero columns.

Theorem 3. $\bar{T}_{n,k}$ is the coefficient of x^n in

$$Z_{\mathcal{A}_k(Z_2)}\ (1+x,\ldots,1+x^{2^n})$$

Theorem 4. T_{nk} is the coefficient of x^n in

$$Z_{\mathcal{A}_k(Z_2)}\ \left(\frac{1}{1-x},\ldots,\frac{1}{1-x^{2^n}}\right)$$

Now, a sample calculation.

$$k=1 \qquad Z_{\mathcal{A}_1(Z_2)} = \frac{1}{2}\left(f_1^2 + f_2\right)$$

$$Z_{\mathcal{A}_1(Z_2)}\ (1+x,1+x^2) = 1 + x + x^2$$

i.e.

$$\bar{T}_{i1} = 1 \qquad \text{for } i=0,1,2$$

$$\sum_{n=0}^{\infty} T_{n1}\, x^n = \frac{1}{2}\left(\frac{1}{(1-x)^2} + \frac{1}{1-x^2}\right)$$

$$T_{n1} = \begin{cases} \dfrac{n+2}{2} & \text{if } n \equiv 0 \bmod 2 \\[2ex] \dfrac{n+1}{2} & \text{if } n \equiv 1 \bmod 2 \end{cases}$$

Suppose n=4, then

$$S_{41} = T_{41} = 3$$

The 16 matrices are partitioned into 3 equivalence classes as shown below:

$$\begin{matrix} [(0000), (1111)] \\ [(0001), (0010), (0100), (1000), (1110), (1101), (1011), (0111)] \\ [(0011), (0101), (0110), (1010), (1001), (1100)] \end{matrix}$$

The calculations for the parameters which Slepian used are not included because of the complexity of the computation. Special computer programs are required to handle this problem.

5-3. Graph Theory

It is perhaps superfluous to mention the connection between this work on Boolean functions and graph theory. Pólya's original paper[30], of over one hundred pages, developed the fundamental theorem and used it to solve many enumeration problems in graph theory. In this section, the connection between the product defined in chapter two and k-colored graphs is shown.

A graph is an ordered pair $< G,R >$ where G is a set (of vertices) and R is a relation on G. aRb holds for $a,b \in G$ iff there is an edge connecting a and b. A k-colored graph is a triple $< G,R,f >$ where G and R are defined as before and f is a function from G <u>onto</u> $Z_k = \{1,2,\ldots,k\}$ such that

$$aRb \Rightarrow f(a) \neq f(b)$$

Two graphs $< G_1,R_1,f_1 >$ and $< G_2,R_2,f_2 >$ are said to be <u>chromatically isomorphic</u> iff there exists an isomorphism θ of the (uncolored) graphs

and a permutation ω of Z_k such that

$$\omega(f_1(a)) = f_2(\theta(a))$$

When the term "the number of k-colored graphs" is used, it is to be understood that we mean the number of chromatically non-isomorphic graphs.

We now specialize to k=2 for bi-colored graphs. Harary has shown that it is sufficient to compute the cycle index of the line group of the complete graphs on mn points with m≠n; symbolically K_{mn}. This group has been shown to be $\mathcal{G}_m \times \mathcal{G}_n$ where $\times$ denotes the Cartesian product of permutation groups.

Turning now to the case where m=n, the line group is larger than $\mathcal{G}_n \times \mathcal{G}_n$ because one can interchange the colors in accordance with the definition of chromatic isomorphism. Harary proved that the line group of K_{nn} is what he called the exponentiation of $\mathcal{I}_2$ and $\mathcal{G}_n$, but what is actually the product defined in chapter two so that the algorithm (theorem 2.2.4) solves some special cases of enumerating bi-colored graphs. Harary has presented an algorithm for the solution of this problem.

5-4. Post Algebras

It seems natural to extend the results which were developed for Boolean algebras to Post algebras. Most of the background can be found in reference [32]. Post functions are defined as mappings from $Z_m^n \rightarrow Z_m$ where, as usual, $Z_m = \{0,1,\ldots,m-1\}$. Thus, there are m^{m^n} Post functions.

First, define $\mathcal{G}_n$ on the variables just as for Boolean functions

v.i.z. for $\sigma \in \mathcal{S}_n$.

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

These permutations of the variables induce permutations of the domain which are automorphisms as before. In fact, the automorphism group of the Post algebra is isomorphic to the symmetric group on m^n letters. Because the mapping which associates with each permutation of the variables a permutation of the domain is a homomorphism, the coefficients of the cycle index are the same as in section 3.5. Clearly, the cycle structure associated with each class is changed. We now calculate the effect of a cycle of length k. A cycle of length k affects m^k domain elements. Consider these elements to be in a one-to-one correspondence with the integers $0,1,\ldots,m^k-1$.

Lemma 1. *If q is any integer such that $0 \leq q \leq m^k-1$, then the least integer d such that*

$$m^d q \equiv q \bmod (m^k-1)$$

must divide k and conversely.

Proof. For the converse, choose $q = \frac{m^k-1}{m^d-1}$. Now let d be the least integer such that $m^d q \equiv q \bmod (m^k-1)$. Then, since $m^k \equiv 1 \bmod (m^k-1)$

$$m^k q \equiv q \bmod (m^k-1)$$

Assume $k = dp + r$ where $0 \leq r < d$

$$m^{dp}\, m^{r} q \equiv q \bmod (m^{k}-1)$$

$$q(m^{d})^{p}\, m^{r} \equiv q \bmod (m^{k}-1)$$

Repeated use of the congruence $m^{d} q \equiv q \bmod (m^{k}-1)$ yields

$$q\, m^{r} \equiv q \bmod (m^{k}-1)$$

which is a contradiction unless r=0.

Theorem 2. A cycle of length k in $\mathfrak{S}_n$ induces permutations on the domain whose lengths are divisors of k and moreover every divisor of k is the length of some cycle.

Proof. One writes the numbers from 0 to $m^{k}-1$ in radix m notation and in order. The effect of a permutation of length k can be obtained by removing the left-hand column and writing it as the right-hand column. This has the effect of multiplying each number by m. Thus, a number q goes successively into mq, $m^{2}q,\ldots,m^{d}q \equiv q \bmod (m^{k}-1)$. Thus, the length of the cycle is the least positive integer d such that

$$m^{d} q \equiv q \bmod (m^{k}-1)$$

Theorem 3. A cycle of length k in $\mathfrak{S}_n$ induces a permutation on the domain whose cycle structure is given by

$$\prod_{d \mid k} f_d^{\,h(d)}$$

where the f_d are the indeterminates of the cycle index and

$$h(p) = \frac{1}{p} \sum_{d \mid p} m^{d} \mu\left(\frac{p}{d}\right)$$

where $\mu(\frac{p}{d})$ is the Möbius function.

Proof. The previous theorem gives the cycle lengths and their multiplicities are given by the requirement

$$\sum_{d|k} d\, h(d) = m^k$$

By the Möbius inversion theorem

$$h(k) = \frac{1}{k} \sum_{d|k} m^d \mu\left(\frac{k}{d}\right)$$

Theorem 4. The cycle index of γ_n as a group on the domain of the Post functions is

$$Z_{\gamma_n} = \frac{1}{n!} \sum_{(j)} \frac{n!}{\prod_{i=1}^{n} j_i!(ij_i)} \times_{i=1}^{n} \left(\prod_{d|i} f_d^{h(d)} \right)^{\times j_i}$$

where the notation $y^{\times j}$ means $\overbrace{y \times y \times \ldots \times y}^{j}$. The number of classes is calculated for a few small values of m and n; this is shown in Table I. It is interesting to note that there are always

$$m^{\binom{n+m-1}{m-1}}$$

transitivity classes consisting of just one function. These are the symmetric Post functions.

TABLE XLVIII

THE NUMBER OF CLASSES OF POST FUNCTIONS UNDER THE SYMMETRIC GROUP

m \ n	1	2	3	4
2	4	12	80	3,984
3	27	10,206	1,271,126,683,458	*
4	256	2,148,007,936	*	*

Turning now to the complementations of the variables there are two different types of complementation used in Post algebras. The first type is shown below.

P	~P
0	1
1	2
2	3
.	
.	
.	
m-2	m-1
m-1	0

Thus, a cyclic permutation is the first analog of complementation. For the complementation of a single variable, the appropriate group is the cyclic group of order m generated by (0,1,...,m-1). The cycle index of this group, $\mathcal{Y}_m$, was given by Pólya as

$$Z_{\mathcal{Y}_m} = \frac{1}{m} \sum_{d|m} \varphi(d)\, f_d^{\frac{m}{d}}$$

where $\varphi(a)$ is the Euler φ function, i.e. the number of integers not exceeding a and relatively prime to a. The cycle index of the group of complementations for n variables, $\mathcal{Y}_m^n$, is now derived.

Theorem 5. The cycle index of $\mathcal{Y}_m^n$ is given by

$$Z_{\mathcal{Y}_m^n} = \frac{1}{m^n} \sum_{d|m} \sum_{t|d} t^n \mu\left(\frac{d}{t}\right) f_d^{\frac{m^n}{d}}$$

Proof. Clearly the structure of the complementation group on the n variables is $\mathcal{Y}_m \times \ldots \times \mathcal{Y}_m$. Thus, it is sufficient to evaluate

$$\bigtimes_{i=1}^{n} \frac{1}{m} \sum_{d|m} \varphi(d)\, f_d^{\frac{m^n}{d}}$$

But this is

$$\frac{1}{m^n} \sum_{d|m} \chi(d,n)\, f_d^{\frac{m^n}{d}}$$

since the cross operation applied to the indeterminants along with the property of LCM's that if $d|m$ and $t|m$, then $< d,t >|m$ gives simply the divisors of m as the cycle lengths. It still remains for us to determine what the coefficient $\chi(d,n)$ is. It is clear that

$$\sum_{d|m} \chi(d,n) = m^n$$

since the sum of the coefficients must be the order of the group. By the Möbius formula

$$\chi(d,n) = \sum_{t|d} t^n \mu(\tfrac{d}{t})$$

It is interesting to note that if m=p, a prime, then this formula reduces to

$$\frac{1}{p^n} (f_1^{p^n} + (p^n-1)\, f_p^{p^{n-1}})$$

which is theorem 3-4.7. The case p=2, is theorem 3-4.6.

Now the second type of complementation which is used in Post algebras is considered. This function is defined by its graph

P	$\neg$P
0	m-1
1	m-2
2	m-3
.	.
.	.
.	.
m-2	1
m-1	0

For $m \equiv 0 \bmod 2$, the associated group has cycle index

$$Z_{\mathcal{G}} = \frac{1}{2}\left(f_1^m + f_2^{\frac{m}{2}}\right)$$

If $m \equiv 1 \bmod 2$, then the cycle index is

$$Z_{\mathcal{G}} = \frac{1}{2}\left(f_1^m + f_1 f_2^{\frac{m-1}{2}}\right)$$

Now we generalize to the case of n variables.

Theorem 6. The cycle index of the complementing group $\mathcal{G}^n$ is

$$\frac{1}{2^n}\left(f_1^{m^n} + (2^n-1)\, f_2^{\frac{m^n}{2}}\right) \quad \text{if } m \equiv 0 \bmod 2$$

$$\frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k} f_1^{m^{n-k}} f_2^{\frac{m^{n-k}(m^k-1)}{2}} \quad \text{if } m \equiv 1 \bmod 2$$

Proof. First we derive the formula if m is even. In that case one can arrive at the result by induction on n. The computation of the induction step is included.

$$Z_{\mathcal{D}^n} = Z_{\mathcal{D}^{n-1}} \times Z_{\mathcal{D}} = \frac{1}{2^{n-1}} \left(f_1^{m^{n-1}} + (2^{n-1}-1)\, f_2^{\frac{m^{n-1}}{2}}\right) \times \frac{1}{2}\left(f_1^m + f_2^{\frac{m}{2}}\right)$$

$$= \frac{1}{2^n} \left(f_1^{m^n} + (2^{n-1}-1)\, f_2^{m^n} + f_2^{\frac{m^n}{2}} + (2^{n-1}-1)\, f_2^{\frac{m^n}{2}}\right)$$

$$= \frac{1}{2^n} \left(f_1^{m^n} + (2^n - 1)\, f_2^{\frac{m^n}{2}}\right)$$

To handle the case where m is odd involves an interesting calculation. Since the cycle indices form a commutative ring under the ordinary addition and the "cross" multiplication, the binomial theorem holds. Thus, when $m \equiv 1 \bmod 2$,

$$\frac{1}{2^n}\left(f_1^m + f_1 f_2^{\frac{m-1}{2}}\right)^{\times n} = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} f_1^{m^{n-k}} \times \left(f_1 f_2^{\frac{m^k-1}{2}}\right)^{\times k}$$

$$= \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} f_1^{m^{n-k}} \times f_1 f_2^{\frac{m^k-1}{2}}$$

$$= \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} f_1^{m^{n-k}} f_2^{\frac{m^{n-k}(m^k-1)}{2}}$$

Q.E.D.

It is now possible to combine the results obtained and form the semi-direct product of these groups and compute the cycle index of this group, but the details are straightforward.

5-5. Sequential Machines

There are many aspects of automata theory to which the present methods apply. Only one application will be discussed, the state assignment problem. Let $\mathcal{A} = < S, \varphi_1, \varphi_2, a >$ be a sequential machine where S denotes the set of internal states, $a \in S$ is the initial state and φ_1 and φ_2 are the direct transition functions. Let $\bar{\bar{S}} = r$.

Definition 1. A state assignment φ is defined as a one-to-one function

$$\varphi: S \to \{0,1\}^k$$

where

$$k \geq - \left[- \log_2 r \right]$$

Certainly two state assignments are equivalent if their images are equivalent under $\mathcal{G}_n$ since permutations and complementations of the range do not change the cost of the assignment. Consider the problem of counting the number of state assignments.

Theorem 2. Let $\mathcal{A} = < S, \varphi_1, \varphi_2, a >$ where $\bar{\bar{S}} = r$. The number of state assignments involving k ($k \geq - \left[-\log_2 r \right]$) bi-stable memory elements (1-1 mappings from S into $\{0,1\}^k$) is given by

$$\frac{d^r}{dz^r} Z_{\mathcal{G}_k} (1+z, 1, \ldots, 1)$$

evaluated at z=0

Proof. This is a special case of theorem 10, section 2-1. where $Z_{\mathcal{G}} = f_1^m$. Note that this result may be written

$$\frac{r!}{2^k\, k!} \sum_{\alpha \in \mathcal{J}_k} \binom{b_1(\alpha)}{r}$$

where $b_1(\alpha)$ is the number of cycles of length one in the permutation α.

Corollary 3. Let $\mathcal{A} = \langle S, \varphi_1, \varphi_2, a \rangle$ where $\bar{\bar{S}} = r$. The number of state assignments involving k states where $k = -\left[-\log_2 r\right]$ is

$$\frac{(2^k-1)\,!}{(2^k-r)!\; k!}$$

Proof. In this case only the identity term in $\mathcal{J}_k$ can contribute to the sum so that the result is

$$\frac{r!}{2^k\, k!} \binom{2^k}{r} = \frac{r!}{2^k\, k!} \frac{2^k!}{r!\; (2^k-r)!}$$

$$= \frac{(2^k-1)!}{(2^k-r)!\; k!}$$

This result was derived in the paper by McCluskey and Unger, reference [24].

Theorem 2 provides a complete solution to the unrestricted counting problem for state assignment. However, the result also counts degenerate state assignments when some state variable is constant over the entire assignment. Also, if $k > -\left[-\log_2 r\right]$ one wishes to divide out by the symmetric group on S. Theorem 2-1.10 may be used in that case to divide out the symmetries on S, but the degeneracy must be handled by special

considerations. Rather than derive the formula, the result which has been obtained by Gilbert is included.

Theorem 4 (Gilbert). The number of non-degenerate state assignments for r states and k bi-stable memory elements is

$$\frac{r!}{k!} \sum_{j=1}^{k} S(k+1,\ j+1)\ 2^{-j}\ \binom{2^j}{r}$$

where S(n,k) are Stirling's numbers of the first kind.

CHAPTER VI

UNSOLVED PROBLEMS

There are a great many problems still to be solved. First, a complete theory of permutation groups involving new "products" which are sufficient to decompose groups which occur in interesting problems needs to be constructed. One also needs necessary and sufficient conditions for the decomposability of such groups along with algorithms for combining the cycle indices of constituent groups to obtain the cycle index of the composite group.

For the practical implementation of our results in switching theory, the group invariance problem must be solved for the following groups

$$\mathcal{L}_2^n$$

$$\mathcal{J}_n$$

$$\mathcal{A}_n(Z_2).$$

Although some partial results are known, complete sets of invariants for these groups on Boolean functions are not yet known. The solution of this problem is facilitated by some recent work of Lechner[21] in preparing a vector space representation of switching functions.

A number of basic enumeration problems are unsolved in automata theory. The number of strongly connected machines is unknown along with the number of equivalence classes of behaviorially equivalent machines. The investigation of the automorphism groups of machines has

just begun, but there is surely a close connection between the structure of the automaton and the structure of its automorphism group. Many of the enumeration problems for automata may be reformulated as problems involving the enumeration of certain types of labelled graphs. This reformulation involved mapping one unsolved problem onto another, as there are still many unsolved problems of this type in graph theory.

It is unknown how many transitive relations of a set of m elements there are. Closely related to this problem is the problem of counting the number of equivalence classes of Boolean connection matrices.

APPENDIX I

CYCLE INDEX POLYNOMIALS FOR $\mathcal{J}_n$

n	$Z_{\mathcal{J}_n}$
1	f_1^2
2	$\frac{1}{2}\left(f_1^4 + f_1^2 f_2\right)$
3	$\frac{1}{6}\left(f_1^8 + 3 f_1^4 f_2^2 + 2 f_1^2 f_3^2\right)$
4	$\frac{1}{24}\left(f_1^{16} + 6 f_1^8 f_2^4 + 3 f_1^4 f_2^6 + 8 f_1^4 f_3^4 + 6 f_1^2 f_2 f_4^3\right)$
5	$\frac{1}{120}\left(f_1^{32} + 10 f_1^{16} f_2^8 + 15 f_1^8 f_2^{12} + 20 f_1^8 f_3^8 + 20 f_1^4 f_2^2 f_3^4 f_6^2 + 30 f_1^4 f_2^2 f_4^6 + 24 f_1^2 f_5^6\right)$
6	$\frac{1}{720}\left(f_1^{64} + 15 f_1^{32} f_2^{16} + 45 f_1^{16} f_2^{24} + 40 f_1^{16} f_3^{16} + 15 f_1^8 f_2^{28} + 120 f_1^8 f_2^4 f_3^8 f_6^4 + 90 f_1^8 f_2^4 f_4^{12} + 40 f_1^4 f_3^{20} + 90 f_1^4 f_2^6 f_4^{12} + 144 f_1^4 f_5^{12} + 120 f_1^2 f_2 f_3^2 f_6^9\right)$

APPENDIX II

CYCLE INDEX POLYNOMIALS FOR $\mathcal{A}_n$

n	$Z_{\mathcal{A}_n}$
n=1	$\frac{1}{2}\left(f_1^2 + f_2\right)$
n=2	$\frac{1}{8}\left(f_1^4 + 3\, f_2^2 + 2\, f_1^2\, f_2 + 2\, f_4\right)$
n=3	$\frac{1}{48}\left(f_1^8 + 13\, f_2^4 + 8\, f_1^2\, f_3^2 + 8\, f_2\, f_6 + 6\, f_1^4\, f_2^2 + 12\, f_4^2\right)$
n=4	$\frac{1}{384}\left(f_1^{16} + 51\, f_2^8 + 48\, f_1^2\, f_2\, f_4^3 + 48\, f_8^2 + 12\, f_1^8\, f_2^4 + 84\, f_4^4 + 12\, f_1^4\, f_2^6 + 32\, f_1^4\, f_3^4 + 96\, f_2^2\, f_6^2\right)$
n=5	$\frac{1}{3840}\left(f_1^{32} + 231\, f_2^{16} + 20\, f_1^{16}\, f_2^8 + 520\, f_4^8 + 80\, f_1^8\, f_3^8 + 720\, f_2^4\, f_6^4 + 160\, f_1^4\, f_2^2\, f_3^4\, f_6^2 + 320\, f_4^2\, f_{12}^2 + 240\, f_1^4\, f_2^2\, f_4^6 + 480\, f_8^4 + 240\, f_2^4\, f_4^6 + 60\, f_1^8\, f_2^{12} + 384\, f_1^2\, f_5^6 + 384\, f_2\, f_{10}^3\right)$
n=6	$\frac{1}{46080}\left(f_1^{64} + 1053\, f_2^{32} + 30\, f_1^{32}\, f_2^{16} + 4920\, f_4^{16} + 180\, f_1^{16}\, f_2^{24} + 160\, f_1^{16}\, f_3^{16} + 5280\, f_2^8\, f_6^8 + 120\, f_1^8\, f_2^{28} + 960\, f_1^8\, f_2^4\, f_3^8\, f_6^4 + 3840\, f_4^4\, f_{12}^4 + 720\, f_1^8\, f_2^4\, f_4^{12} + 5760\, f_8^8 + 2160\, f_2^8\, f_4^{12} + 640\, f_1^4\, f_3^{20} + 1920\, f_2^2\, f_6^{10} + 1440\, f_1^4\, f_2^6\, f_4^{12} + 2304\, f_1^4\, f_5^{12} + 6912\, f_2^2\, f_{10}^6 + 3840\, f_1^2\, f_2\, f_3^2\, f_6^9 + 3840\, f_4\, f_{12}^5\right)$

APPENDIX III

CYCLE INDEX POLYNOMIALS FOR $GL_n(Z_2)$

n	$Z_{GL_n(Z_2)}$
1	f_1^2
2	$\frac{1}{6}\left(f_1^4 + 3 f_1^2 f_2 + 2 f_1 f_3\right)$
3	$\frac{1}{168}\left(f_1^8 + 21 f_1^4 f_2^2 + 42 f_1^2 f_2 f_4 + 56 f_1^2 f_3^2 + 48 f_1 f_7\right)$
4	$\frac{1}{20160}\left(f_1^{16} + 105 f_1^8 f_2^4 + 210 f_1^4 f_2^6 + 1260 f_1^4 f_2^2 f_4^2 + 2520 f_1^2 f_2 f_4^3 + 112 f_1 f_3^5 + 1680 f_1 f_3 f_6^2 + 1120 f_1^4 f_3^4 + 3360 f_1^2 f_2 f_3^2 f_6 + 5760 f_1^2 f_7^2 + 1344 f_1 f_5^3 + 2688 f_1 f_{15}\right)$
5	$\frac{1}{9,999,360}\left(f_1^{32} + 465 f_1^{16} f_2^8 + 26,040 f_1^8 f_2^4 f_4^4 + 312,480 f_1^4 f_2^2 f_4^6 + 624,960 f_1^2 f_2 f_4^3 f_8^2 + 6510 f_1^8 f_2^{12} + 78,120 f_1^4 f_2^6 f_4^4 + 19,840 f_1^8 f_3^8 + 416,640 f_1^4 f_2^2 f_3^4 f_6^2 + 833,280 f_1^2 f_2 f_3^2 f_4 f_6 f_{12} + 55,552 f_1^2 f_3^{10} + 833,280 f_1^2 f_3^2 f_6^4 + 476,160 f_1^4 f_7^4 + 1,428,480 f_1^2 f_2 f_7^2 f_{14} + 952,320 f_1 f_3 f_7 f_{21} + 666,624 f_1^2 f_5^6 + 1,333,248 f_1^2 f_{15}^2 + 1,935,360 f_1 f_{31}\right)$

$$Z_{GL_6(Z_2)} = \frac{1}{20,158,709,760}\Big(f_1^{64} + 1953\, f_1^{32} f_2^{16} + 468,720\, f_1^{16} f_2^{8} f_4^{8}$$

$$+ 26,248,320\, f_1^{8} f_2^{4} f_4^{12} + 314,979,840\, f_1^{4} f_2^{2} f_4^{6} f_8^{4}$$

$$+ 629,959,680\, f_1^{2} f_2 f_4^{3} f_8^{6} + 136,710\, f_1^{16} f_2^{24} + 9,843,120\, f_1^{8} f_2^{12} f_4^{8}$$

$$+ 91,869,120\, f_1^{4} f_2^{6} f_4^{12} + 234,360\, f_1^{8} f_2^{28} + 333,312\, f_1^{16} f_3^{16}$$

$$+ 34,997,760\, f_1^{8} f_2^{4} f_3^{8} f_6^{4} + 419,973,120\, f_1^{4} f_2^{2} f_3^{4} f_4^{2} f_6^{2} f_{12}^{2}$$

$$+ 839,946,240\, f_1^{2} f_2 f_3^{2} f_4^{3} f_6 f_{12}^{3} + 69,995,520\, f_1^{4} f_2^{6} f_3^{4} f_6^{6}$$

$$+ 34,283,520\, f_1^{8} f_7^{8} + 719,953,920\, f_1^{4} f_2^{2} f_7^{4} f_{14}^{2}$$

$$+ 1,439,907,840\, f_1^{2} f_2 f_4 f_7^{2} f_{14} f_{28} + 223,985,664\, f_1^{4} f_5^{12}$$

$$+ 671,956,992\, f_1^{2} f_2 f_5^{6} f_{10}^{3} + 447,971,328\, f_1^{4} f_{15}^{4}$$

$$+ 1,343,913,984\, f_1^{2} f_2 f_{15}^{2} f_{30} + 3,901,685,760\, f_1^{2} f_{31}^{2}$$

$$+ 447,971,328\, f_1 f_3^{3} f_5^{3} f_{15}^{3} + 895,942,656\, f_1 f_3 f_{15}^{4}$$

$$+ 422,830,080\, f_1 f_7^{9} + 1,919,877,120\, f_1^{2} f_3^{2} f_7^{2} f_{21}^{2}$$

$$+ 18,665,472\, f_1^{4} f_3^{20} + 279,982,080\, f_1^{4} f_3^{4} f_6^{8}$$

$$+ 839,946,240\, f_1^{2} f_2 f_3^{2} f_6^{9} + 111,104\, f_1 f_3^{21} + 34,997,760\, f_1 f_3^{5} f_6^{8}$$

$$+ 419,973,120\, f_1 f_3 f_6^{2} f_{12}^{4} + 719,953,920\, f_1 f_7 f_{14}^{4}$$

$$+ 1,919,877,120\, f_1 f_{63} + 319,979,520\, f_1 f_9^{7} + 639,959,040\, f_1 f_{21}^{3}$$

$$+ 55,996,416\, f_1^{2} f_2 f_3^{10} f_6^{5}\Big)$$

APPENDIX IV

CYCLE INDEX POLYNOMIALS FOR $\mathcal{A}_n(Z_2)$

n	$Z_{\mathcal{A}_n(Z_2)}$
1	$\frac{1}{2} f_1^2 + f_2$
2	$\frac{1}{24} f_1^4 + 3 f_2^2 + 6 f_1^2 f_2 + 6 f_4^2 + 8 f_1 f_3$
3	$\frac{1}{1344} f_1^8 + 49 f_2^4 + 42 f_1^4 f_2^2 + 252 f_4^2 + 168 f_4^2 + 168 f_1^2 f_2 f_4$ $+ 384 f_1 f_7 + 224 f_1^2 f_3^2 + 224 f_2 f_6$
4	$\frac{1}{322,560} f^{16}_1 + 645 f_2^8 + 210 f_1^8 f_2^4 + 1,344 f^4_4 + 840 f_1^4 f_2^6 +$ $+ 5,040 f_1^4 f_2^2 f_4^2 + 5,040 f_2^4 f_4^2 + 20,160 f_1^2 f_2 f_4^3 + 20,160 f_8^2$ $+ 1792 f_1 f_3^5 + 26,880 f_1 f_3 f_6^2 + 26,880 f_1^2 f_2 f_3^2 f_6$ $+ 4480 f_1^4 f_3^4 + 13,440 f_2^2 f_6^2 + 46,080 f_1^2 f_7^2 + 46,080 f_2 f_{14}$ $+ 43,008 f_1 f_{15} + 21,504 f_1 f_5^3$
5	$\frac{1}{319,979,520} f^{32}_1 + 32,581 f^{16}_2 + 930 f^{16}_1 f_2^8 + 2,455,200 f_4^8$ $+ 104,160 f_1^8 f_2^4 f_4^4 + 312,480 f_2^8 f_4^4 + 2,499,840 f_1^4 f_2^2 f_4^6$ $+ 3,888,640 f_2^4 f_6^4 + 14,999,040 f_8^4 + 9,999,360 f_1^2 f_2 f_4^3 f_8^2$ $+ 26,040 f_1^8 f_2^{12} + 624,960 f_1^4 f_2^6 f_4^4 + 79,360 f_1^8 f_3^8$ $+ 3,333,120 f_1^4 f_2^2 f_3^4 f_6^2 + 19,998,720 f_4^2 f_{12}^2$ $+ 13,332,480 f_1^2 f_2 f_3^2 f_4 f_6 f_{12} + 888,832 f_1^2 f^{10}_3$ $+ 14,221,312 f_2 f_6^5 + 13,332,480 f_1^2 f_3^2 f_6^4 + 3,809,280 f_1^4 f_7^4$

$$5 \quad + 11,427,840\, f_2^2\, f_{14}^2 + 22,855,680\, f_1^2\, f_2\, f_7^2\, f_{14} + 22,855,680\, f_4\, f_{28}$$

$$+ 30,474,240\, f_1\, f_3\, f_7\, f_{21} + 10,665,984\, f_1^2\, f_5^6 + 10,665,984\, f_2\, f_{10}^3$$

$$+ 21,331,968\, f_1^2\, f_{15}^2 + 21,331,968\, f_2\, f_{30} + 61,931,520\, f_1\, f_{31}$$

$$+ 2,499,840\, f_2^4\, f_4^6 \Big)$$

APPENDIX V

HARARY'S DEFINITION OF THE EXPONENTIATION GROUP

In this appendix, we shall review Harary's definition of the exponentiation of two groups[15]. It will be shown that this group product does not occur as the structure of $\mathcal{J}_n$ as Harary has suggested.

Let $X = \{x_1, \ldots, x_a\}$ and let $\mathcal{A}$ be a permutation group of degree a and order m acting on X. Let $\mathcal{B}$ be a group of order n and degree b acting on object sety Y. Then consider Y^X, the class of all functions from X to Y. The group $\mathcal{B}^{\mathcal{A}}$ is constructed* by first permuting a domain object by $\alpha \in \mathcal{A}$ and then permuting the images in Y for each domain element by elements of $\mathcal{B}$. More precisely, if $\gamma \in \mathcal{B}^{\mathcal{A}}$, then for $f \in Y^X$,

$$\gamma f = \beta_i f(\alpha x_i) \qquad i=1,\ldots,a.$$

This is Harary's definition. Table XLVIX summarizes the pertinent parameters of Harary's group.

---

*The symbol $\mathcal{B}^{\mathcal{A}}$ denotes the group constructed here and is Harary's original notation. In chapter II, the same notation is used for a different group. No confusion will result because the use of Harary's group is confined to this appendix.

	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{B}^{\mathcal{A}}$
Object set	X	Y	Y^X
Degree	a	b	b^a
Order	m	n	$m \cdot n^a$

TABLE XLVIX

THE PROPERTIES OF $\mathcal{B}^{\mathcal{A}}$

Now we shall show that Harary's claim that $\mathcal{OJ}_n$ is permutationally equivalent to $\mathcal{Y}_2 \wr \mathcal{S}_n$ must be false. We have noted in the past that $\mathcal{OJ}_n$ must be of degree 2^n, i.e. it is a permutation group on the domain only. Thus, Harary must want to take the degree of $\mathcal{S}_n$ to be n and the degree of $\mathcal{Y}_2$ to be 2. The n objects which $\mathcal{S}_n$ permutes are, of course, the integers 1,...,n. But this means that the object set of $\mathcal{Y}_2 \wr \mathcal{S}_n$ is the class of all mappings of 1,...,n into $\{0,1\}$, but these objects are not the Boolean functions of n variables, nor are they the domain of the Boolean functions.

The only other possible interpretation of Harary's statement is that he wants the degree of $\mathcal{Y}_2$ to be 2 and the degree of $\mathcal{S}_n$ to be 2^n, i.e. $\mathcal{S}_n$ defined on the domain. Now this is reasonable, but it points out the fundamental error since, in this case, the order of $\mathcal{Y}_2 \wr \mathcal{S}_n$ would be $n! \, 2^{2^n}$ which is not the order of $\mathcal{OJ}_n$.

Explicitly then, Harary's mistake was to define the β_i as mappings on the range when, in fact, they are mappings on the n individual sets $\{0,1\}$ which comprise the domain.

APPENDIX VI

DERIVATION OF THEOREM 2.2.4

The derivation of $Z_{\mathcal{J}_n}$ provides some of the background for the present proof. We shall use the fact that $\gamma_n \otimes \mathcal{S}$ is isomorphic to the complete monomial group of degree n of $\mathcal{S}$ (cf. Ore [28]). It was previously shown (in the derivation of $Z_{\mathcal{J}_n}$) that it is sufficient to consider a cycle of the form $\beta = (0,\ldots,0,\alpha)\ (1,\ldots,k)$ where, $\alpha^p = 1$ (Cf. Ore [28], theorem 7.) We shall now derive the cycle structure induced by this term. In the process of the derivation, Ore's theorems 4 and 5 will be strengthened slightly.

Clearly the canonical term has order kp. The cycle lengths must divide kp and their LCM must be kp. Suppose $d \mid kq$ for $q < p$, then $\beta^{k(p-1)}(d) = d = (\alpha^{p-1},\ldots,\alpha^{p-1})\ (d)$. The assumption that the terms in $Z_{\mathcal{S}}$ have no fixed points insures that every digit of the radix m expansion of d is changed, so d is not invariant under $\beta^{k(p-1)}$. The argument for the converse is given similarly to the derivation of the cycle structure of $Z_{\mathcal{J}_n}$. Thus, the cycle structure corresponding to $\sigma = (1,2,\ldots,k)$ is

$$\frac{1}{g} \sum_{p} b_p \prod_{\substack{d \mid kp \\ d \nmid kq \\ q<p}} f_d^{\,e_k(d)}$$

The exponents may be calculated recursively as Slepian did or by by deriving a generalized version of the Möbius formula. The latter approach yields

$$e_k(lp) = \frac{1}{lp} \sum_{\substack{d \mid kp \\ d \nmid kq \\ q < p}} m^{\frac{d}{p}} \mu\left(\frac{kp}{d}\right)$$

BIBLIOGRAPHY

1. Artin, E., Geometric Algebra, Interscience Publishers, Inc., New York (1957).

2. Ashenhurst, R. L., "The application of counting techniques," Proceedings of the Association of Computing Machinery, Pittsburgh Meeting (1952), pp. 293-305.

3. Burnside, Theory of Groups of Finite Order, Cambridge University Press, 2nd edition (1911).

4. Caldwell, S. H., Switching Circuits and Logical Design, John Wiley and Sons, Inc., New York (1958).

5. Church, R., "Tables of irreducible polynomials for the first four prime moduli," Annals of Mathematics, Vol. 36, No. 1, January (1935), pp. 198-209.

6. Davis, R. L., "The number of structures of finite relations," Proceedings of the American Mathematical Society, Vol. 4 (1953) pp. 486-495.

7. DeBruijn, N. G., "Generalization of Pólya's fundamental theorem in enumerative combinatorial analysis," Koninklijke Nederlandse Akademie Van Wetenschappen, Series A, Vol. LXII, No. 2 (1959), pp. 59-69.

8. Dickson, L. E., Linear Groups with an Exposition of the Galois Field Theory, Dover Publications, New York (1958).

9. Dunham, B., Middleton, D., North, J., Sleter, J., and Weltzien, J., "The multi-purpose bias device. Part II. The efficiency of logical elements," IBM Journal of Research and Development, Vol. 3, No. 1 (1950), pp. 46-53.

10. Elspas, B., "Autonomous linear sequential networks," IRE Transactions, CT-6, March (1959), pp. 45-60.

11. Elspas, B., "Self-complementary symmetry types of Boolean functions," IRE Transactions of Electronic Computers, Vol. EC-9, No. 2 (1960), pp. 264-266.

12. Golomb, S., "On the classification of Boolean functions," IRE Transactions on Information Theory, Vol. IT-5 (1959), pp. 176-186.

13. Golomb, S. W., "A mathematical theory of discrete classification," Information Theory, Butterworth (1961), pp. 404-425.

14. Hall, M., Theory of Groups, The Macmillan Co., New York, 1959.

15. Harary, F., "Exponentiation of permutation groups," American Mathematical Monthly, Vol. 66, No. 7, August-September (1959).

16. Harary, F., "On the number of bi-colored graphs," Pacific Journal of Mathematics, Vol. 8, No. 4 (1958), pp. 743-755.

17. Harvard Computation Laboratory, Synthesis of Electronic Computing and Control Circuits, Harvard University Press, Cambridge, Massachusetts (1951).

18. Hellerman, L., Equivalence Classes of Logical Functions, IBM Technical Publication TR00.819, November (1961).

19. Higgonet, and Grea, Logical Design of Electrical Circuits, McGraw Hill Book Company, New York (1958).

20. Klein, F., Vergleichende Betrachtungen über nuere geometriche Forschungen, Erlangen (1872).

21. Lechner, R., Affine Equivalence of Switching Functions, Thesis Abstract, Harvard University (1963).

22. Lorens, C. S., Invertible Boolean Functions, Space General Corporation Report, July 1 (1962).

23. Mautner, F. I., "An extension of Klein's Erlanger program; Logic as invariant theory," American Journal of Mathematics, Vol. 68 (1946), pp. 345-384.

24. McClusky, and Unger, "A note on the number of internal variable assignments for sequential switching circuits," IRE Transactions, Vol. EC-8, No. 4, December (1958).

25. Nechiporuk, E. I., "On the synthesis of networks using linear transformations of variables," Doklady Akad. Nauk 123: 610-12, No. 4, December (1958). Available in English in Automation Express, April (1959), pp. 12-13.

26. Ninomiya, I., "On the number of genera of Boolean functions of n variables," Memoirs of the Faculty of Engineering of Nagoya University, Vol. 11, No. 1-2, pp. 54-58.

27. Ninomiya, I., "On the number of types of symmetric Boolean output matrices," Memoirs of the Faculty of Engineering of Nagoya University, Vol. 7, November (1955), pp. 115-124.

28. Ore, O., "Theory of monomial groups," Transactions of the American Mathematical Society, Vol. 51 (1942), pp. 15-64.

29. Peterson, W. W., Error Correcting Codes, John Wiley and Sons, New York (1961).

30. Pólya, G., "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen," Acta Mathematica, Vol. 68 (1937), pp. 145-253.

31. Pólya, G., "Sur les types des propositions composées," Journal of Symbolic Logic, Vol. 5 (1940), pp. 98-103.

32. Post, E. L., "A general theory of elementary propositions," American Journal of Mathematics, Vol. 43, pp. 163-185.

33. Povarov, G. N., "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), pp. 74-94.

34. Sagalovich, I. U., "On the number of types of symmetry for contact (1,k)-pole networks," Doklady Akad. Nauk. 130: 72-73, No. 1, January (1960); available in English in Automation Express, March (1960), pp. 39-40.

35. Seshu, and Reed, Graph Theory and Electrical Networks, Addison Wesley Company, Inc., Reading, Massachusetts (1961).

36. Shannon, C. E., "A symbolic analysis of relay and switching circuits," AIEE Transactions, Vol. 57, pp. 713-723 (1938).

37. Shannon, C. E., "The synthesis of two-terminal switching circuits," The Bell System Technical Journal, Vol. 28 (1949), pp. 59-98.

38. Sikorski, R., Boolean Algebras, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 25, Springer-Verlag, Berlin (1960).

39. Singer, T., "The theory of counting techniques," Proceedings of the Association for Computing Machinery, Pittsburgh Meeting (1952), pp. 287-291.

40. Slepian, D., "On the number of symmetry types of Boolean functions of n variables," Canadian Journal of Mathematics, Vol. 5 (1953), pp. 185-193.

41. Slepian, D., "Some further theory of group codes," The Bell System Technical Journal, Vol. XXXIX, No. 5, September (1960), pp. 1219-1252.

42. Weyl, H., Classical Groups, Princeton University Press, Princeton, New Jersey (1946).