Electronics Research Laboratory
University of California
Berkeley, California

THE NUMBER OF SYMMETRY TYPES OF POST FUNCTIONS

by

Michael A. Harrison

This research was initiated at the University of Michigan, under support of the Aeronautical Systems Division, Wright-Patterson Air Force Base (Contract No. AF 33(657)-7811), and was completed at the University of California, under support of the Air Force Office of Scientific Research of the Office of Aerospace Research, the Dept. of the Army, Army Research Office, and the Dept. of the Navy, Office of Naval Research (Grant No. AF-AFOSR-139-63).

August 9, 1963

ABSTRACT

Five groups are discussed which naturally classify Post functions into transitivity sets. Since all the groups discussed are subgroups of the automorphism group of the Post algebra, the resulting classification into symmetry types preserves the structure of the functions.

In all cases the number of classes is obtained and asymptotic estimates are given.

I. INTRODUCTION

There are a variety of ways of classifying the formulae of m-valued logics. In this paper transformations on the truth functions will induce a classification of the formulae.

Historically, both Jevons[6] and Clifford[2] considered the problem of classifying propositional functions into equivalence classes in a natural way. It was Pólya[10] who systematically posed the problem of counting the number of classes under the group of complementations and permutations and who gave the correct numerical answers for functions of four or fewer variables. It was Slepian,[14] however, who first solved the general problem of counting the number of equivalence classes for an arbitrary number of variables. In the paper by Harrison[5] a new method of obtaining Slepian's result is given which uses the structure of the groups involved in a more systematic manner.

In the present paper the results for Boolean functions are generalized to Post algebras.

We now sketch an introduction to the theory of Post algebras. More details can be found in Refs. 11, 12, and 13.

Definition 1.1 Let $Z_m = \{0, \ldots, m-1\}$ and define a Post function to be any mapping from Z_m^n into Z_m where $Z_m^n = Z_m \times \ldots \times Z_m$ (n times).

The formulae of m-valued logic are built up in the usual way by induction.

Definition 1. 2.

a) 0, ..., m-1 are Post formulae.
b) x_i (i = 1, ..., n) is a Post formula.
c) If A is a Post formula, then $\sim A$ is a Post formula.
d) If A is a Post formula, then $\neg A$ is a Post formula.
e) If A, B are Post formulae, then AB is a Post formula.

f) If A, B are Post formulae, then $A \vee B$ is a Post formula.

g) The only Post formulae are as given in (a-f).

As usual, the interpretation is given by a mapping from the formulae into the truth values.

Definition 1. 3. An assignment is defined as a mapping α from $X = \{x_1, \ldots, x_n\}$ into Z_m. The valuation mapping with respect to an assignment α is defined as a mapping $|\ |_\alpha$ recursively as follows:

a) $|0|_\alpha = 0, \ldots, |m-1|_\alpha = m-1$

b) $|x_i|_\alpha = \alpha(x_i)$ for $i = 1, \ldots, n$

c) $|\sim A|_\alpha = m-1 - |A|_\alpha$

d) $|\neg A|_\alpha = \begin{cases} |A|_\alpha + 1 & \text{if } |A_\alpha| \neq m-1 \\ 0 & \text{if } |A_\alpha| = m-1 \end{cases}$

e) $|AB|_\alpha = \min(|A|_\alpha, |B|_\alpha)$

f) $|A \vee B|_\alpha = \max(|A|_\alpha, |B|_\alpha)$

Thus two Post formulae P and Q are called equivalent, written $P \equiv Q$, if and only if for every assignment α, $|P|_\alpha = |Q|_\alpha$.

There is a one-to-one mapping which associates with every Post formula P the corresponding Post function. The appropriate map is

$$|P| = \bigcup_\alpha (\alpha, |P|_\alpha)$$

It is clear that $|P|$ is a mapping from Z_m^n into Z_m and in fact preserves the operations on formulae.

Definition 1. 4. The system $\mathcal{P}_{m,n} = \langle P_{m,n}; \ldots, \vee, \sim, \neg, 0, \ldots, m-1 \rangle$ is a Post algebra on n generators. The natural equivalence relation on $\mathcal{P}_{m,n}$ is given by $\equiv$. $P_{m,n}$ is the set of formulae generated from $0, 1, \ldots, m-1$ and $x_1, \ldots, x_n$ by means of Definition 1. 2.

The mapping $P \to |P|$ maps the algebra of Post formulae onto the

free algebra of m^{m^n} Post functions. The map also suggests how to define operations on the Post functions so that the systems are isomorphic.

Definition 1.5. Define the following operations on Post functions:

$$(f \vee g)(a) = \max(f(a), g(a))$$

$$(fg)(a) = \min(f(a), g(a))$$

$$\sim f(a) = m-1-f(a)$$

$$\neg f(a) = \begin{cases} f(a)+1 & \text{if } f(a) \neq m-1 \\ 0 & \text{if } f(a) = m-1 \end{cases}$$

Proposition 1.6. The Post algebra $\mathcal{P}_{m,n} = \langle P_{m,n}, \vee, \cdot, \sim, \neg, 0, \ldots, m-1 \rangle$ is isomorphic to the free algebra of Post functions. $\mathcal{F}_{m,n} = \langle F_{m,n}, \vee, \cdot, \sim, \neg, 0, \ldots, m-1 \rangle$.

Proof. Consider the map. $|\ |: P \to |P|$. If $P \equiv Q$, then $|P| = |Q|$ so $|\ |$ is a map from equivalence classes of Post formulae to Post functions. The map is onto by the canonical form theorem (Cf. Rosser and Turquette,[13] Theorem 2.5). Clearly, the operations are preserved.

Next we characterize the automorphisms of $\mathcal{F}_{m,n}$.

Definition 1.7. An automorphism α of $\mathcal{F}_{m,n}$ is a one-to-one map from $F_{m,n}$ onto $F_{m,n}$ such that for Post functions f and g,

$$\alpha(f \vee g) = \alpha(f) \vee \alpha(g)$$

$$\alpha(fg) = (\alpha f)(\alpha g)$$

$$\alpha(\sim f) = \sim \alpha(f)$$

$$\alpha(\neg f) = \neg \alpha(f)$$

Theorem 1.8. The automorphism group of $\mathcal{F}_{m,n}$ is isomorphic to the symmetric group of degree m^n, $\mathfrak{S}_{m^n}$.

Proof. Clearly any automorphism α must fix the constant functions 0, ..., m-1. Express f in expanded normal form.

$$f(x_1, \ldots, x_n) = \bigvee_{i_1=0}^{m-1} \cdots \bigvee_{i_n=0}^{m-1} J_{i_1}(x_1) \cdots J_{i_n}(x_n)\, f(i_1, \ldots, i_n)$$

Since α is an automorphism,

$$\alpha f = \bigvee_{i_1=0}^{m-1} \cdots \bigvee_{i_n=0}^{m-1} \alpha\left(J_{i_1}(x_1) \cdots J_{i_n}(x_n)\right)\, f(i_1, \ldots, i_n)$$

As the i_j range over their respective values, the $J_1(x_1) \ldots J_i(x_n)$ are in one-to-one correspondence with the domain elements of Z_m^n and hence α is a permutation of the domain. Conversely, any permutation of the domain induces a permutation of the terms of the expanded normal form. Such a correspondence is easily seen to be an automorphism.

A similar result is given by Mautner[7] for Boolean algebras.

II. PÓLYA'S THEOREM

The counting results to be obtained will be consequences of the famous theorem of Pólya.

Let $\mathcal{F}$ be the class of all functions from a finite set D to a finite set R. Suppose D has s elements and the $\mathcal{G}$ is a permutation group of degree s and order g acting on D. Two functions $f_1, f_2 \in \mathcal{F}$ 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 $R(\bar{\bar{R}} = q)$ 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. Pólya'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 $i=1, \ldots, r$.

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 multivariate 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 Pólya's theorem, we must develop the concept of the cycle index polynomial of $\mathcal{OJ}$ (zyklenzeiger), denoted by $Z_{\mathcal{OJ}}$. 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 $\mathcal{OJ}$ 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

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

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 equivalance classes to the determination of the figure series and the cycle index polynomial.

Theorem 2.1. (Pólya). The configuration counting series is obtained by substituting the figure counting series into the cycle index polynomial of

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

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.

Corollary 2.2. The total number of equivalence classes of functions $f: D \to R$ under a group $\mathcal{J}$ of order g and degree s is

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

where q is the cardinality of R.

III. PRODUCTS OF PERMUTATION GROUPS

In combinatorial analysis, one often defines products of permutation groups. It is then essential to be able to derive the cycle index of the composite group in terms of the cycle indices of the constituent groups. In this section two such products are considered.

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

Definition 3.1. The direct product of two groups written $\mathcal{A} \times \mathcal{B}$ is defined on the object set $X \times Y$ in the following way $(\alpha, \beta)(x, y) = \big(\alpha(x), \beta(y)\big)$.

Thus, the order of $\mathcal{A} \times \mathcal{B}$ is mn and the degree is ab. 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

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

The following theorem was stated by Harary.

Theorem 3.2. $Z_{\mathcal{A} \times \mathcal{G}} = Z_{\mathcal{A}} \times Z_{\mathcal{G}}$ where the cross operation for polynomials is defined as follows:

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

where the cross operation on indeterminates is defined as

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

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

where $<p, q>$ 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

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

and

$$Z_{\mathfrak{S}_3} = \frac{1}{6} (h_1^3 + 3h_1 h_2 + 2h_3)$$

be the cycle indices for the symmetric group on two and three letters,

respectively. We compute

$$Z_{\mathfrak{S}_2 \times \mathfrak{S}_3} = \frac{1}{12}\Big((g_1^2 \times h_1^3) + 3(g_1^2 \times h_1 h_2) + 2(g_1^2 \times h_3)$$

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

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

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

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

Proof. It is easily verified that the cross operation on indeterminates 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 $\langle p, q\rangle$ 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.

The next operation to be defined has an interesting history. In an attempt to abstract Slepian's solution[14] of the problem of counting the symmetry types of Boolean functions of n variables, Harary[3] constructed a product of permutation groups called the exponentiation. As indicated in appendix V of 4, Harary's construction is not the right one to characterize the symmetry group of Boolean functions.

A new group product will be formulated which will characterize Slepian's result and will find applications in a variety of situations. Let $\mathcal{S}$ be a group of order g acting on object set X. The degree of $\mathcal{S}$ 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 $\mathcal{A} \otimes \mathcal{S}$ will now be defined. It is convenient to think of the 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 $\mathcal{A} \otimes \mathcal{S}$ 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 $\mathcal{S}$ (not necessarily distinct), the i^{th} column is to be permuted by β_i for $i=1, \ldots, a$. The abstract structure of $\mathcal{A} \otimes \mathcal{S}$ is the semi-direct product of $\mathcal{A}$ by $\mathcal{S}^a$ where $\mathcal{S}^a$ denotes $\mathcal{S} \times \ldots \times \mathcal{S}$.

In the case described where $\mathcal{A}$ is the symmetric group, $\mathcal{G}_n \times \mathcal{S}$ has the abstract structure of the complete monomial group of degree n of $\mathcal{S}$. The theory of such groups has been worked out by Ore[8] and reference to several of his theorems will be made. For the purposes of this paper, it will be sufficient to derive the cycle index of $\mathcal{G}_n \otimes \mathcal{S}$ where $\mathcal{S}$ has a restricted type of cycle structure. The condition on $\mathcal{S}$ can be expressed by requiring that $Z_{\mathcal{S}}$ is of the form

$$Z_{\mathcal{S}} = \frac{1}{g} \sum_{(k)} b_{(k)} f_1^r f_k^s.$$

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

Theorem 3.3. Let $\mathcal{G}_n$ be the group induced by the symmetric group of degree n and let $\mathcal{S}$ be a group of degree m and order g whose cycle index has terms whose structure is of the form $f_1^r f_k^s$.

$$Z_{\mathcal{G}_n \otimes \mathcal{S}} = \frac{1}{n! g^n} \sum_{(j)} \frac{n! g^n}{\prod_{i=1}^{n} j_i! (gi)^{j_i}} \prod_{i=1}^{n} \left(\sum_{(k)} b_{(k)} f_1^r \prod_{\substack{d \mid ik \\ d \nmid pi \\ p<k}} f_d^{g(d)} \right)^{x_{j_i}}$$

where

$$g(ik) = \frac{1}{ik} \sum_{\substack{d \mid ik \\ d \nmid pk \\ p<i}} \left(m^{d/i} - r \right) \mu\left(\frac{ik}{d}\right)$$

and $\mu(a)$ is the Möbius function. y^{Xj} denotes $\overbrace{yX\ldots Xy}^{j}$, and the sum is over all partitions of n.

The previous theorem is proved in Ref. 4, and structural results about monomial groups are derived there. A summary of these results will be presented in section VIII.

IV. ENUMERATION IN POST ALGEBRA

The groups to be studied are now introduced along with the generalities of the way in which this class of groups operates on the Post algebras.

The first allowable transformation will be to complement the variables of a particular function by repeated applications of the operation $\neg$. For example, we will say that $f(x_1, x_2, x_3)$ is equivalent to $f(x_1, \neg x_2, \neg\neg x_3)$. More precisely we have the following formal definition.

Definition 4.1. Let Σ_m denote the cyclic group of order m generated by the cycle $(0, \ldots, m\text{-}1)$ and Σ_m^n denote the direct product of n copies of Σ_m. Σ_m^n is defined as an operator group on Post functions in the following way. For any $(\varphi_1, \ldots, \varphi_n) \in \Sigma_m^n$ where $\varphi_j \in \Sigma_m$ for $j=1, \ldots n$, and for any $f(x_1, \ldots, x_n) \in F_{m,n}$, define

$$(\varphi_1, \ldots, \varphi_n)\ f(x_1, \ldots, x_n) = f(\varphi_1 x_1, \ldots, \varphi_n x_n)$$

where

$$\varphi_i x_i = \begin{cases} x_i+1 & \text{if } x_i \neq m\text{-}1 \\ 0 & \text{if } x_i = m\text{-}1 \end{cases}$$

The same construction is also employed for the second kind of complementation.

Definition 4. 2. Let $\mathcal{D}_m$ denote a permutation group of order two defined on Z_m whose non-identity map δ has the property

$$\delta : \quad a \rightarrow m\text{-}1\text{-}a$$

Define $\mathcal{D}_m^n$ to be the direct product of n copies of $\mathcal{D}_m$. $\mathcal{D}_m^n$ operates on Post functions by the following construction

$$(\delta_1, \ldots, \delta_n)\ f(x_1, \ldots, x_n) = f(\delta_1(x_1), \ldots, \delta_n(x_n))$$

Thus $\mathcal{L}_m^n$ corresponds to allowing all complementations of the variables x_i $(i=1, \ldots, n)$ by $\sim$ while $\mathcal{D}_m^n$ allows all possible complementations by $\neg$.

In a sense, the most natural group* defined on Post functions is the symmetric group of degree n, $\mathcal{S}_n$, operating on the variables.

Definition 4. 3. We define the symmetric group as an operator group on Post functions by

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

for any $f \in \mathcal{F}_{m,n}$ and any $\sigma \in \mathcal{S}_n$.

Note that a Post function f is <u>symmetric</u> if $\sigma f = f$ for all $\sigma \in \mathcal{S}_n$.

The symmetric Post functions can be studied from this point of view as suggested in Ref. 7.

Definition 4. 4. Let $\mathcal{M}_m^n$ denote the least group containing $\mathcal{S}_n$ and $\mathcal{L}_m^n$ while $\mathcal{H}_m^n$ denotes the least group containing $\mathcal{S}_n$ and $\mathcal{D}_m^n$.

---

*Cf. Mautner[7].

It will be seen later that $\mathcal{O}_m^n$ and $\mathcal{B}_m^n$ have the structure of the monomial representation of Σ_m and $\mathcal{V}_m$ respectively.

The relations of these groups to one another are summarized by Fig. 1 which represents part of the lattice of subgroups of $\mathfrak{S}_m n$.

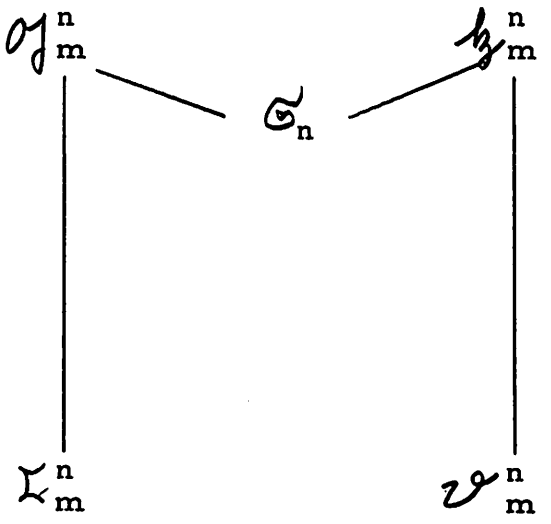

Fig. 1

The general enumeration problem which we shall solve is the following. We have a group, say $\mathcal{O}$, defined on the variables or generators x_i of $\mathcal{F}_{m,n}$. Any $\gamma \in \mathcal{O}$ permutes the variables of $\mathcal{F}_{m,n}$. The permutation of the variables, γ, induces in a natural way, a permutation h_γ of the domain of the Post functions. h_γ induces, by theorem 1.8, an automorphism α_γ of $\mathcal{F}_{m,n}$. Fig. 2 illustrates the situation.

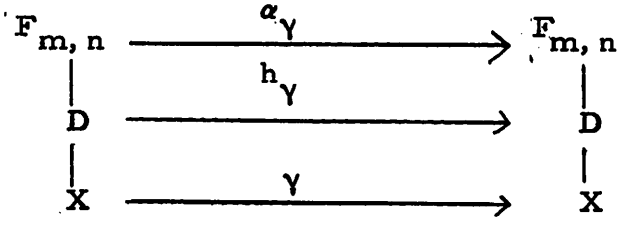

Fig. 2

The present situation is a direct generalization of the results of Harrison[5] which handled the case where $m=2$.

V. THE GROUP Σ_m^n

The group Σ_m^n is the direct product of n copies of Σ_m.

It is well known (cf. Pólya[9]) that the cycle index of Σ_m is given by

$$Z_{\Sigma_m} = \frac{1}{m} \sum_{d|m} \varphi(d)\, f_d^{m/d}$$

where $\varphi(d)$ is the Euler φ function, i.e., the number of integers not exceeding d and relatively prime to d.

Theorem 5.1. The cycle index of Σ_m^n is given by

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

Proof. Since the structure of the complementation group on the n variables is $\Sigma_m \times \ldots \times \Sigma_m$, it is sufficient to evaluate

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

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 indeterminates along with the property of least common multiples that if $d|m$ and $t|m$, then $\langle d, t\rangle | m$ gives simply the divisors of m as the cycle lengths. It still remains 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

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

It is interesting to note that if $m=p$, a prime, then the theorem reduces to

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

which is given in Harrison.[5] The case $p=2$ was studied by Ashenhurst.[1]

Corollary 5.2. The number of classes of Post functions in $\mathcal{F}_{m,n}$ under $\mathcal{Y}_m^n$ is given by

$$\frac{1}{m^n} \sum_{d|m} \sum_{t|d} t^n \mu(\frac{d}{t}) \, m^{\frac{m^n}{d}}$$

Proof. Cf. Corollary 2.2.

VI. THE GROUP $\mathcal{V}_m^n$

The group of complementations by $\neg$ has a very simple cycle index.

Lemna 5.1. If $m \equiv 0 \mod 2$, then

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

If $m \equiv 1 \pmod 2$, then

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

Proof. The non-identity element of $\mathcal{D}_m$ has order two.

Again, the result for the direct product is derived by using the cross operation.

Theorem 5.2. If $m \equiv 0 \pmod 2$, then

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

Proof. The argument is an induction on n.

Basis n=1. The result is given by lemma 5.1.

Induction step.

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

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

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

Theorem 5.3. If $m \equiv 1 \pmod 2$, then

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

Proof. Since the cycle index polynomials form a commutative ring under the ordinary addition and the "cross" multiplication, the binomial theorem holds. Thus

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

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

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

Corollary 5.5. The number of equivalence classes of functions in $\mathcal{F}_{m,n}$ under $\mathcal{G}_m^n$ is

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

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

Note that the case $m=2$ reduces to the proper result for Boolean algebras as it should.

VII. THE GROUP $\mathfrak{S}_n$

It is possible to derive the cycle index for $\mathfrak{S}_n$ operating on $\mathfrak{F}_{m,n}$ in a way exactly analagous to the derivation for Boolean algebra as is done in Harrison.[5] The details of the proof for Post algebras carried out in Ref. 4.

It is much easier to observe that $\mathfrak{S}_n$ is permutationally equivalent to $\mathfrak{S}_n \otimes \mathfrak{I}$ where $\mathfrak{I}$ is the identity group of degree one. Thus

$$Z_{\mathfrak{I}} = f_1$$

Theorem 7.1. The cycle index of $\mathfrak{S}_n$ as an operator group on $\mathfrak{F}_{m,n}$ is

$$Z_{\mathfrak{S}_n} = \frac{1}{n!} \sum_{(j)} \frac{n!}{\prod_{i=1}^{n} j_i! i^{j_i}} \prod_{i=1}^{n} \left(\prod_{d|i} f_d^{h(d)} \right)^{X^{j_i}}$$

where the notation y^{X^j} means $\overbrace{yX \ldots Xy}^{j}$. The sum is over all non-negative rational integer solutions. $(j) = (j_1, \ldots j_n)$ of $\sum_{i=1}^{n} i j_i = n$ and

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

Proof. By theorem 3.3. $Z_{\mathfrak{S}_n}$ equals the expression shown. The exponents must satisfy

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

By the Möbius inversion formula.

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

Example: n=3

$$Z_{\mathfrak{S}_3} = \frac{1}{6} \left((f_1^3)^{X3} + 3f_1^3 X f_1^3 f_2^3 + 2f_1^3 f_3^8 \right)$$

$$= \frac{1}{6} \left(f_1^{27} + 3f_1^9 f_2^9 + 2f_1^3 f_3^8 \right)$$

Corollary 7.2. The number of equivalence classes of $\mathcal{F}_{m,n}$ under $\mathfrak{S}_n$ is

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

where $h_{j_k}(i_k) = \frac{1}{i_k} \sum_{d|i_k} m^{dj_k} \mu(\frac{i_k}{d})$ for $k=1,\ldots,n$ and $(i_1,\ldots,i_n)$ denotes the greatest common divisor of $i_1,\ldots,i_n$. The sum is over all partitions of n.

Proof. In Ref. 4 it is shown how to rewrite the previous theorem as

$$Z_{\mathfrak{S}_n} = \frac{1}{n!} \sum_{(j)} \frac{n!}{\prod_{i=1}^{n} j_i!\, i^{j_i}} \prod_{i_1|1} \cdots \prod_{i_n|n} f_{\langle i_1,\ldots,i_n \rangle}^{(i_1,\ldots,i_n)\, h_{j_1}(i_1) \cdots h_{j_n}(i_n)}$$

where $h_{j_k}(i_k) = \frac{1}{i_k} \sum_{d|i_k} m^{dj_k} \mu(\frac{i_k}{d})$ for $k=1,\ldots,m$. $\langle i_1,\ldots,i_n \rangle$ and $(i_1,\ldots,i_n)$ denote the least common multiple and greatest common

divisors if $i_1, \ldots, i_n$, respectively. From this result and Corollary 2. 2, the present theorem follows.

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 I. 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	*	*

VIII. THE GROUP $\mathcal{O}_m^n$

The group $\mathcal{O}_m^n$ is to be the least group containing Σ_m^n and $\mathfrak{S}_n$. The group can be constructed by forming a set of ordered pairs (α, σ) where $\alpha \in \Sigma_m^n$ and $\sigma \in \mathfrak{S}_n$. The group is defined as follows on Post functions where $\alpha \in \Sigma_m^n$ and $\sigma \in \mathfrak{S}_n$.

$$(\alpha, \sigma)\ f = f(\alpha_1(x_{\sigma(1)}), \ldots, \alpha_n(x_{\sigma(n)}))$$

Theorem 8.1 $\mathcal{G}_m^n = \left\{ (\alpha, \sigma) \,\middle|\, \alpha \in \Sigma_m^n, \ \sigma \in \mathfrak{S}_n \right\}$

is a group under the following operation

$$(\alpha_1, \sigma_1)\ (\alpha_2, \sigma_2) = (\alpha_1 \cdot \sigma(\alpha_2),\ \sigma_1\sigma_2)$$

where $\cdot$ denotes the group operation of Σ_m^n and

$$\sigma(\alpha_2) = \sigma(\alpha_{21}, \ldots, \alpha_{2n}) = (\alpha_{2\,\sigma(1)}, \ldots, \alpha_{2\,\sigma(n)})$$

Proof. First we verify that the operation is associative.

$$\begin{aligned}
&((\alpha_1, \sigma_1)(\alpha_2, \sigma_2))(\alpha_3, \sigma_3) \\
&= ((\alpha_1 \cdot \sigma_1(\alpha_2)),\ \sigma_1\sigma_2)(\alpha_3, \sigma_3) \\
&= (\alpha_1 \cdot \sigma_1(\alpha_2) \cdot \sigma_1\sigma_2(\alpha_3),\ \sigma_1\sigma_2\sigma_3)
\end{aligned}$$

Now we compute

$$\begin{aligned}
&(\alpha_1, \sigma_1)((\alpha_2, \sigma_2)(\alpha_3, \sigma_3)) \\
&= (\alpha_1, \sigma_1)(\alpha_2 \cdot \sigma_2(\alpha_3),\ \sigma_2\sigma_3) \\
&= (\alpha_1 \cdot \sigma_1(\alpha_2 \cdot \sigma_2(\alpha_3)),\ \sigma_1\sigma_2\sigma_3) \\
&= (\alpha_1 \cdot \sigma_1(\alpha_2) \cdot \sigma_1\sigma_2(\alpha_3),\ \sigma_1\sigma_2\sigma_3)
\end{aligned}$$

Note that we used the fact that $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta)$. The verification of the rest of the group axioms is routine.

Lemma 8.2.

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

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

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

Where 0 denotes the indentity of $\sum_m^n$ and 1 denotes the identity of $\mathfrak{S}_n$.

Lemma 8.3. For $\sigma \in \mathfrak{S}_n$ and $\alpha \in \sum_m^n$, the mapping $\varphi_\sigma : \alpha \longrightarrow \sigma(\alpha)$ is an automorphism of $\sum_m^n$.

Proof: Clearly φ_σ is a map from $\sum_m^n$ into $\sum_m^n$. The map is onto, since given any $\alpha \in \sum_m^n$, $\sigma^{-1}(\alpha)$ maps onto α under φ_σ. Suppose $\sigma(\alpha) = \sigma(\beta)$, then $\alpha = \sigma^{-1}(\sigma(\alpha)) = \sigma^{-1}(\sigma(\beta)) = \beta$ and φ_σ is one-to-one. Suppose $\alpha \longrightarrow \sigma(\alpha), \beta \longrightarrow \sigma(\beta)$, then $\alpha \cdot \beta \longrightarrow \sigma(\alpha \cdot \beta)$

$$\begin{aligned}\sigma(\alpha \cdot \beta) &= \sigma(\alpha_1 \cdot \beta_1, \ldots, \alpha_n \cdot \beta_n) \\ &= (\alpha_{\sigma(1)} \cdot \beta_{\sigma(1)}, \ldots, \alpha_{\sigma(n)} \cdot \beta_{\sigma(n)}) \\ &= \sigma(\alpha) \cdot \sigma(\beta)\end{aligned}$$

and φ_σ is an automorphism.

In group theory, this process of combining $\sum_m^n$ and $\mathfrak{S}_n$ to form $\mathcal{G}_m^n$ is a special case of forming the semi-direct product of

$\mathcal{Y}_m^n$ by $\mathcal{S}_n$. The following theorem is a special case of the theorem which characterizes the semi-direct product.[4]

Theorem 8.4. $\mathcal{O}_m^n$ is the semi-direct product of $\mathcal{Y}_m^n$ by $\mathcal{S}_n$. The elements of the type $(0, \sigma)$ form a subgroup isomorphic to $\mathcal{S}_n$ while the elements of the type $(i, 1)$ form a normal subgroup isomorphic to $\mathcal{Y}_m^n$. Furthermore, $\mathcal{Y}_m^n \cap \mathcal{S}_n = (0,1)$ and $\mathcal{Y}_m^n \cup \mathcal{S}_n = \mathcal{O}_m^n$. The order of $\mathcal{O}_m^n$ is $n!m^n$.

Proof. All the stated properties are obvious except perhaps the normality of $\mathcal{O}_m^n$. This follows directly from Lemma 2.

Lemma 8.5. The group $\mathcal{O}_m^n$ is permutationally equivalent to $\mathcal{S}_n \otimes \mathcal{Y}_m$.

Proof. The map is (α, σ)

$$\longrightarrow \left((\alpha_1, \ldots, \alpha_n), \sigma \right) \qquad \text{where } \alpha_i \in \mathcal{Y}_m$$

Theorem 8.6. The cycle index of $\mathcal{O}_m^n$ is

$$\frac{1}{n!m^n} \sum_{(j)} \frac{n!m^n}{\prod_{i=1}^{n} j_i!(mi)^{j_i}} \prod_{i=1}^{n} \left(\sum_{d \mid m} \varphi(d) \prod_{\substack{t \mid id \\ t \nmid pi \\ p<d}} f_t^{e(t)} \right)^{x_i^{j_i}}$$

where the sum is over the partitions of n, $\varphi(d)$ is the Euler φ-function

and

$$e(ik) = \frac{1}{ik} \sum_{\substack{d \mid ik \\ d \nmid pk \\ p<i}} m^{\frac{d}{i}} \mu(\tfrac{ik}{d})$$

Proof. Theorem 3.2 gives the form of the result. Note that if $d \mid ik$, but $d \nmid pk$ for any $p<i$., then $i \mid d$. Thus the non-zero terms will be cycle lengths which are multiples of i. Thus

$$\sum (id)g(id) = m^k$$

or

$$g(ik) = \frac{1}{ik} \sum_{\substack{d \mid ik \\ d \nmid pk \\ p< i}} m^{\frac{d}{i}} \mu(\tfrac{ik}{d})$$

by a mild generalization of the Möbius inversion formula.

Example. $m = 3,\ n = 2$

$$\frac{1}{2 \cdot 3^2} \left((f_1^3 + 2f_3)^{\times 2} + 3(f_1^3 f_2^3 + 2f_3 f_6) \right)$$

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

The number of classes is computed for a few values of m and n in Table II.

Table II. The Number of Classes of Post Functions under $\mathcal{G}_m^n$

m \ n	1	2	3	4
2	3	6	22	402
3	11	1, 230	94, 186, 271, 892	*
4	70	134, 355, 076	*	*

IX. THE GROUP $\mathcal{H}_m^n$

The process of constructing $\mathcal{H}_m^n$ is so similiar to the construction of $\mathcal{G}_m^n$ that only an outline is given.

Lemma 9.1. $\mathcal{H}_m^n$ is permutationally equivalent to $\mathfrak{S}_n \otimes \mathcal{P}_m$.

Theorem 9.2. The cycle index of $\mathcal{H}_m^n$ is given by

$$\frac{1}{n!2^n} \sum_{(j)} \frac{n!2^n}{\prod_{i=1}^{n} j_i!(2i)^{j_i}} \times_{i=1}^{n} \left(\prod_{d \mid i} f_d^{e(d)} + f_1^{\delta} \prod_{\substack{d \mid 2i \\ d \nmid i}} f_d^{g(d)} \right)^{x^{j_i}}$$

where $\delta = \begin{cases} 0 \text{ if } m \equiv 0 \bmod 2 \\ 1 \text{ if } m \equiv 1 \bmod 2. \end{cases}$ The sum is over all partitions of n.

$e(d) = \frac{1}{k} \sum_{d \mid k} m^d \mu(\frac{k}{d})$ and $g(2k) = \frac{1}{2k} \sum_{\substack{d \mid 2k \\ d \nmid k}} (m^{d/2} - \delta) \mu(\frac{2k}{d})$.

Proof. See Theorem 3.3

The results of some computations are presented in Table III.

Table III. The Number of Equivalence Classes in $\mathcal{F}_{m,n}$ under $\mathcal{B}_m^n$

m \ n	1	2	3	4
2	3	6	22	402
3	18	2,862	158,949,223,533	*
4	136	537,157,696	*	*

X. LOWER BOUNDS AND ASYMPTOTIC ESTIMATES

It is easy to give a lower bound on the number of equivalence classes which is also asymptotic to the number of classes for large n.

Theorem 10.1. A lower bound on the number of equivalence classes of functions in $\mathcal{F}_{m,n}$ is given by

$$m^{m^n - n} \quad \text{for } \mathcal{L}_m^n$$

$$\frac{m^{m^n}}{2^n} \quad \text{for } \mathcal{V}_m^n$$

$$\frac{m^{m^n}}{n!} \quad \text{for } \mathcal{S}_n$$

$$\frac{m^{m^n - n}}{n!} \quad \text{for } \mathcal{O}_m^n$$

$$\frac{m^{m^n}}{n!2^n} \quad \text{for } \mathcal{B}_m^n$$

Proof. Replace the polynomial by only the term corresponding to the identity mapping.

Corollary 10.2 The number of classes is asymptotic to the lower bounds given in Theorem 10.1.

Proof. The order of all the groups studied satisfy the hypothesis of the following lemma.

Lemma 10.3. If $\mathcal{G}$ is any group whose order $g < 2^{m^{n-1}(m-\frac{1}{2})\log_2 m - \epsilon \log_2 n}$ for any $\epsilon > 0$, then the number of transitivity classes in $\mathcal{F}_{m,n}$ under $\mathcal{G}$ is asymptotic to $\frac{m^{m^n}}{g}$.

Proof. The number of classes is equal to

$$\frac{1}{g}(m^{m^n} + \theta)$$

where θ represents the remainder of the cycle index polynomial. The maximum value of θ is

$$(g-1)m^{\frac{m^{n-1}}{2}}$$

Thus

$$\frac{\frac{g-1}{g}\, m^{\frac{m^{n-1}}{2}}}{\frac{m^{m^n}}{g}} = \frac{(g-1)}{m^{m^{n-1}(m-\frac{1}{2})}} < \frac{g}{m^{m^{n-1}(m-\frac{1}{2})}} < \frac{1}{n^{\epsilon}} = o(1)$$

Hence, the number of classes is

$$\frac{1}{g}(m^{m^n} + \theta) = \frac{1}{g}\, m^{m^n} + o\left(\frac{m^{m^n}}{g}\right) \sim \frac{m^{m^n}}{g}$$

XI. CONCLUSIONS

Applications of the present results can be made to the theory of switching, but these applications are immediate in light of the theorems of Ref. 4 which require only a knowledge of the cycle index polynomials of the appropriate groups and these have now been constructed.

REFERENCES

1. Ashenhurst, R. L., "The Application of Counting Techniques," Proc. Assn. of Computing Machinery, Pittsburgh Meeting (1952), pp. 293-305.
2. Clifford, W. K., Mathematical Papers, (London 1882), pp. 1-16.
3. Harary, F., "Exponentiation of Permutation Groups," Amer. Math. Monthly, Vol. 66, No. 7; Aug.-Sept. (1959).
4. Harrison, M. A., Combinatorial Problems in Boolean Algebras and Applications to the Theory of Switching, University of Michigan Ph. D. Dissertation; June 1963.
5. Harrison, M. A., "The Number of Transitivity Sets of Boolean Functions," SIAM Journal; September 1963.
6. Jevon, W. S., The Principles of Science, London, 2nd Ed., 1892.
7. Mautner, F. I., "An Extension of Klein's Erlanger Program; Logic as Invariant Theory," Amer. Jour. of Math., Vol. 68 (1946), pp. 345-384.
8. Ore, O., "Theory of Monomial Groups," Trans. Amer. Math. Soc., Vol. 51 (1942), pp. 15-64.
9. Pólya, G., "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und Chemische Verbindungen," Acta Mathematica, Vol. 68 (1937), pp. 145-253.
10. Pólya, G., "Sur les Types des Propositions Composées," Jour. of Symbolic Logic, Vol. 5 (1940), pp. 98-103.
11. Post, Emil L., "Introduction to a General Theory of Elementary Propositions," Amer. Jour. of Math., 43 (1921), pp. 163-185.
12. Rosenbloom, Paul C., The Elements of Mathematical Logic, Dover, New York (1950), esp. pp. 51-54.
13. Rosser, J. Barkley, and Turquette, A. R., Many-Valued Logics. Studies in Logic and the Foundations of Mathematics, North Holland Publishing Co., Amsterdam (1951), esp. 27-48.
14. Slepian, D., "On the Number of Symmetry Types of Boolean Functions of n Variables," Can. Jour. of Math., Vol. 5 (1953), pp. 185-193.