THE UNIVERSITY OF MICHIGAN

COLLEGE OF ENGINEERING
Department of Electrical Engineering
Information Systems Laboratory

Technical Note

THE NUMBER OF CLASSES OF INVERTIBLE BOOLEAN FUNCTIONS

Michael A. Harrison

ORA Project 04879

under contract with:

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

administered through:

OFFICE OF RESEARCH ADMINISTRATION ANN ARBOR

July 1962

SUMMARY

In a recent paper, C. S. Lorens[4] has focused attention on invertible Boolean functions. Lorens has counted the number of classes of such functions by considering the same group acting on both the domain and range of such functions.

In this work, we give an algorithm for obtaining Lorens' results and extend his work to allow different groups on the domain and range.

I. INTRODUCTION

The work of C. S. Lorens[4] has focused attention on the invertible Boolean functions. 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 we are considering one-to-one onto mappings of $\{0,1\}^n$ into $\{0,1\}^n$. These are just the $2^n!$ permutations of $\{0,1\}^n$.

Lorens has counted the number of classes of such functions when one allows the same group to operate on the domain and on the range. These results will be generalized in this paper.

Three different groups will be considered as transformation groups on Boolean functions. $\mathcal{C}_2^n$ will denote the group of all 2^n complementations of the variables; $\mathcal{S}_n$ will denote the group of all n! permutations of the variables, and $\mathcal{G}_n$ denotes the least group containing both $\mathcal{C}_2^n$ and $\mathcal{G}_n$. The order of $\mathcal{G}_n$ is of course $n!2^n$. In order to carry out our calculations we shall use a combinatorial result due to De Bruijn.[2]

II. DE BRUIJN'S THEOREM

Consider a class of functions from a finite domain D to a finite range R. Let $\mathcal{G}$ and $\mathcal{H}$ denote permutation groups acting on D and R respectively. Two functions f_1 and f_2 are called equivalent if and only if there exist elements $\alpha \in \mathcal{G}$ and $\beta \in \mathcal{H}$ such that $f_1(d) = \beta f_2(\alpha(d))$ for all $d \in D$. This equivalence relation decomposes the family of all functions into equivalence classes. We desire the number of such classes.

The statement of the pertinent theorem will require the cycle index polynomial of a group. Let $\mathfrak{G}$ be a permutation group of order g and degree s. Let $f_1,\ldots,f_s$ be s indeterminates and let $g_{j_1,\ldots,j_s}$ be the number of permutations of $\mathfrak{G}$ having j_k cycles of length k for $k = 1,2,\ldots,s$. Naturally

$$\sum_{i=1}^{s} i j_i = s \tag{1}$$

Then the cycle index of $\mathfrak{G}$ is defined as

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

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

It is now possible to state the theorem of De Bruijn which we shall use.

Theorem 2.1. <u>The number of classes of one-to-one functions is</u>

$$Z_{\mathfrak{G}}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_2}\right) Z_{\mathfrak{H}}(1 + z_1,\ 1 + 2z_2,\ldots,1 + sz_s)$$

<u>evaluated at $z_1 = z_2 = \ldots = z_s = 0$.</u>

It is clear that before proceeding we shall need to know the cycle indices for Σ_2^n, $\mathfrak{M}_n$, and $\mathfrak{G}_n$. Ashenhurst[1] first calculated the cycle index for Σ_2^n while Slepian[5] first counted the classes under $\mathfrak{G}_n$. The explicit polynomials are given in Reference 3 and the result is quoted below without proof.

Theorem 2.2.

$$Z_{\Sigma_2^n} = \frac{1}{2^n}\left(f_1^{2^n} + (2^n - 1) f_2^{2^{n-1}}\right)$$

$$Z_{\mathcal{Y}_n} = \frac{1}{n!}\sum_{(j)} \frac{n!}{\prod_{k=1}^{n} j_k!\,k^{j_k}} \mathop{\times}_{i=1}^{n} \left(\prod_{d|i} f_d^{e(d)}\right)^{j_i}$$

$$Z_{\mathcal{O}_n} = \frac{1}{n!2^n}\sum_{(j)} \frac{n!}{\prod_{k=1}^{n} j_k!\,k^{j_k}} \mathop{\times}_{i=1}^{n} \left(\prod_{d|i} f_d^{e(d)} + \prod_{\substack{d\nmid i\\ d|2i}} f_d^{g(d)}\right)^{j_i}$$

<u>where the last two cycle indices are summed over all partitions of n such that</u> $\sum_{i=1}^{n} i j_i = n$. The functions e(d) and g(d) along with the cross operation (x) are defined in Reference 3.

III. APPLICATIONS

The following lemma will facilitate our calculations.

Lemma 3.1. <u>A term of the form</u>

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

<u>yields</u>

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

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.

We will first apply this lemma to the case where Γ_2^n acts on both the domain and the range.

Theorem 3.2. <u>The number of classes with Γ_2^n acting on both the range and the domain is given by</u>

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

The calculations for the other cases have been carried out and are summarized below. 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. These answers agree with those of Lorens except in the case $n = 4$ with the symmetric group on both the range and the domain.

Since we are dealing with invertible functions, the results with $\mathfrak{G}$ acting on the domain and $\mathfrak{H}$ acting on the range are exactly the same as with $\mathfrak{H}$ and $\mathfrak{G}$ interchanged.

n	Number of Invertible Functions	$\mathcal{L}_2^n$ on Range and Domain	γ_n^{ν} on Range and Domain	$\mathcal{T}_n$ on Range and Domain
1	2	1	2	1
2	24	6	7	2
3	40,320	924	1,172	52
4	20,922,789,888,000	81,738,720,000	36,325,278,240	142,090,700

n	$\mathcal{L}_2^n$ on Domain, γ_n^{μ} on Range	$\mathcal{L}_2^n$ on Domain, $\mathcal{T}_n$ on Range	γ_n^{μ} on Domain, $\mathcal{T}_n$ on Range
1	1	1	1
2	3	3	2
3	840	196	154
4	54,486,432,000	2,271,124,800	2,270,394,624

IV. ACKNOWLEDGMENT

I wish to thank Dr. B. Elspas for pointing out the work of Lorens and suggesting this problem.

REFERENCES

1. Ashenhurst, R. L., "The application of counting techniques," *Proceedings of the Association for Computing Machinery*, Pittsburgh Meeting (1952), pp. 293-305.

2. De Bruijn, 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.

3. Harrison, M. A., *The Number of Transitivity Sets of Boolean Functions*, The University of Michigan Technical Note 04879-3-T, June 1962.

4. Lorens, C. S., *Invertible Boolean Functions*, Space-General Corporation Research Memorandum No. 21, January 1962.

5. Slepian, D., "On the number of symmetry types of Boolean functions of n variables, *Canadian Journal of Mathematics*, Vol. 5 (1953), pp. 185-193.