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 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 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. $L_2^n$ will denote the group of all $2^n$ complementations of the variables; $\mu_n$ will denote the group of all $n!$ permutations of the variables, and $\sigma_\mathcal{F}_n$ denotes the least group containing both $L_2^n$ and $\mu_n$. The order of $\sigma_\mathcal{F}_n$ is of course $n!2^n$. In order to carry out our calculations we shall use a combinatorial result due to De Bruijn.

II. DE BRUIJN'S THEOREM

Consider a class of functions from a finite domain $D$ to a finite range $R$. Let $\sigma_\mathcal{F}$ and $\mu_\mathcal{R}$ 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 $\alpha \in \sigma_\mathcal{F}$ and $\beta \in \mu_\mathcal{R}$ 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 $\mathcal{G}$ be a permutation group of order $g$ and degree $s$. Let $f_1, \ldots, f_s$ be $s$ indeterminates and let $g_{j_1}, \ldots, g_{j_s}$ be the number of permutations of $\mathcal{G}$ having $j_k$ cycles of length $k$ for $k = 1, 2, \ldots, s$. Naturally

$$\sum_{l=1}^{s} l j_l = s$$  \hspace{1cm} (1)

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

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

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. The number of classes of one-to-one functions is

$$Z_{\mathcal{G}} \left( \frac{d}{dz_1}, \ldots, \frac{d}{dz_s} \right) Z_f (1 + z_1, 1 + 2z_2, \ldots, 1 + sz_s)$$

evaluated at $z_1 = z_2 = \ldots = z_s = 0$.

It is clear that before proceeding we shall need to know the cycle indices for $\mathcal{G}_n$, $\mathcal{F}_n$, and $\mathcal{G}_n$. Ashenhurst\(^1\) first calculated the cycle index for $\mathcal{G}_n$ while Slepian\(^5\) first counted the classes under $\mathcal{G}_n$. The explicit polynomials are given in Reference 3 and the result is quoted below without proof.
Theorem 2.2.

\[
Z \sum_{n=2}^{\infty} \left( \frac{1}{n^n} \left( f_1^{2^n} + (2^n - 1) f_2^{2^n-1} \right) \right)
\]

\[
Z \mu_n = \frac{1}{n!} \sum_{(j)} \frac{n!}{\prod_{k=1}^{n} j_k!} \prod_{i=1}^{n} \left( \prod_{d \mid i} f_d^{e(d)} \right)^{j_i}
\]

\[
Z \sigma_n = \frac{1}{n!} \sum_{(j)} \frac{n!}{\prod_{k=1}^{n} j_k!} \prod_{i=1}^{n} \left( \prod_{d \mid i} f_d^{e(d)} + \prod_{d \mid 21} f_d^{g(d)} \right)^{j_i}
\]

where the last two cycle indices are summed over all partitions of \( n \) such that \( \sum_{i=1}^{n} ij_i = n \). 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. A term of the form

\[
\left[ a \left( \frac{\partial^{m_1}}{\partial z_{1}^{i_1}} \cdots \frac{\partial^{m_s}}{\partial z_{s}^{i_s}} \right) b(1+k_1z_{k_1})^{j_1} \cdots (1+k_sz_{k_s})^{j_s} \right] z_1 = z_2 = \ldots = z_s = 0
\]

yields

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

We will first apply this lemma to the case where \( \sum_{2}^{n} \) acts on both the domain and the range.

**Theorem 3.2.** The number of classes with \( \sum_{2}^{n} \) acting on both the range and the domain is given by

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

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 \( \sigma f \) acting on the domain and \( f \) acting on the range are exactly the same as with \( f \) and \( \sigma f \) interchanged.
<table>
<thead>
<tr>
<th>n</th>
<th>Number of Invertible Functions</th>
<th>( \sum_{x=2}^{n} ) on Range and Domain</th>
<th>( \nu_n ) on Range and Domain</th>
<th>( \sigma_f ) on Range and Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>24</td>
<td>6</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>40,320</td>
<td>924</td>
<td>1,172</td>
<td>52</td>
</tr>
<tr>
<td>4</td>
<td>20,922,789,888,000</td>
<td>81,738,720,000</td>
<td>36,325,278,240</td>
<td>142,090,700</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>( \sum_{x=2}^{n} ) on Domain</th>
<th>( \sum_{x=2}^{n} ) on Domain</th>
<th>( \nu_n ) on Domain</th>
<th>( \sigma_f ) on Domain</th>
<th>( \sigma_f ) on Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>840</td>
<td>196</td>
<td>154</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>54,486,432,000</td>
<td>2,271,124,800</td>
<td>2,270,394,624</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IV. ACKNOWLEDGMENT

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


