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

COLLEGE OF ENGINEERING
Department of Electrical Engineering
Information Systems Laboratory

Technical Note

ON THE CLASSIFICATION OF BOOLEAN FUNCTIONS BY THE GENERAL LINEAR AND AFFINE GROUPS

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

September 1962

SUMMARY

The general linear group and the affine group of transformations are defined over the field of two elements and are applied as transformation groups to Boolean functions. Algorithms for counting the number of classes under both groups are derived. The concept of equivalence is extended by allowing complementation of the range of the functions and the number of such classes is also obtained. The number of classes of invertible Boolean functions is calculated when these groups are considered. Some other problems are stated and solved.

1. INTRODUCTION

Let $\mathcal{F}_n$ denote the free Boolean algebra on n generators consisting of the 2^{2^n} functions from $\{0,1\}^n$ into $\{0,1\}$; also let $Z_2 = \{0,1\}$ be the field of two elements which must be of characteristic two. By $GL_n(Z_2)$, we 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 $f(x_1,\ldots,x_n) \in \mathcal{F}_n$. We define the product Af as

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

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

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

We shall call two functions f and g equivalent if and only if there exists a matrix $A \in GL_n(Z_2)$ such that $f(\underset{\sim}{x}) = g(\underset{\sim}{x}A)$ for all $\underset{\sim}{x}$. This clearly defines an equivalence relation on $\mathcal{F}_n$ which decomposes $\mathcal{F}_n$ into disjoint transitivity

classes. The first problem to be posed is the determination of the number of classes.

2. THE NUMBER OF CLASSES UNDER $GL_n(Z_2)$

Using the celebrated theorem of Pólya[15] to count the number of classes, it is sufficient to construct the cycle index polynomial of $GL_n(Z_2)$ where we take a representation of this group of degree 2^n. That is, it suffices to know the behavior of the group on the atoms of $\mathcal{J}_n$. The cycle index is discussed in detail in references 15,2,7,8,9, and 10 to which the reader is referred.

We shall confine ourselves to a presentation of the algorithm. All of the available information necessary to calculate the cycle index is available in the literature. Dickson[4] (page 235) calculates the coefficients of the cycle index which are essentially the number of elements in a conjugacy class. Elspas[5] derives and Slepian[18] uses the cycle structure for each class. Slepian[18] has solved related problems in counting the number of classes of codes under $GL_n(Z_2)$.

Our algorithm 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. We shall imagine the irreducible polynomials sorted by degree and ennumerated. The polynomial $p(x) = x$ will be excluded from all our considerations. We 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[3] has listed irreducible polynomials for the first four prime moduli. Table I indicates the first 22 poly-

nomials along with values of d_i and e_i for Z_2.

TABLE I

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

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 irredicible 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.

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

where $\mu\left(\frac{n}{d}\right)$ is the Möbius function. Because we are ignoring the polynomial $p(x) = x$, 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 II shows the first few values of $I(n)$ and t_n. Of course

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

TABLE II

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 our 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

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, we introduce two final definitions. Let $q_{ij} = e_i 2^{b_j}$ where $b_j = -[-\log_2 j]$. $[x]$ 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

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

where the cross operation is defined as follows

$$\left(\prod_{p=1}^{r} a_p^{i_p}\right) \times \left(\prod_{q=1}^{s} b_q^{j_q}\right) = \prod_{p,q}\left(a_p^{i_p} \times b_q^{j_q}\right)$$

where

$$a_p^{i_p} \times b_q^{j_q} = f^{i_p j_q}{}^{(p,q)}_{\langle p,q\rangle}$$

and $\langle p,q\rangle$ is the least common multiple of p and q; (p,q) is the greatest common divisor of p and q. $\times$ is an associative and commutative operation. The sum is over all classes.*

Proof. The complicated coefficient is merely the number of elements in the class as given by Dickson.[4] The products of f's denote the cycle structure as derived by the Elspas.[5]

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, cf. 8. The results are given in Table III.

TABLE III

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

*Since the symbol f^k is ambiguous and might mean $\overbrace{f\ldots f}^{k}$ or $\overbrace{f\times\ldots\times f}^{k}$, we write $f^{\times k}$ in the latter case.

If we replace each indeterminate f_i by $1 + x^i$ and collect all the terms into a polynomial in x, then Pólya's theorem insures us that the coefficient of x^k is the number of functions with k atoms in their normal form expansion. The results are collected in Table IV where N_n^k denotes this number while T_n denotes the total number of classes.

TABLE IV

k \ n	N_n^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

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 $N_n^4 = 5$

It is desirable to examine the structure of the equivalence classes themselves. We now mention a few considerations which 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 $j^{\underline{th}}$ column to the $i^{\underline{th}}$ 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 $j \neq i$.*

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

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

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

3. THE NUMBER OF CLASSES UNDER THE AFFINE GROUP

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

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

*This argument also shows that the class $\mathcal{L}_n$ 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.

where $A \in GL_n(Z_2)$ and b is a vector whose components $b_i \in Z_2$ for $i = 1,\ldots,n$. $\oplus$ denotes componentwise addition modulo 2. We denote the affine group by $\mathcal{AL}_n(Z_2)$. The effect of the affine group is the complementation of those variables of the Boolean function for which $b_i = 1$. The order of $\mathcal{AL}_n(Z_2)$ is

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

In an obvious way, the action of $\mathcal{AL}_n(Z_2)$ decomposes the functions into equivalence classes. We shall now count the number of classes. The problem has been solved by Neckiporuk[14] but his proof has not been published. The subgroup of the affine group consisting of translations only is the well known group Γ_2^n of 2 and 8. 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 $\mathcal{AL}_n(Z_2)$ as a permutation group is $\Gamma_2^{GL_n(Z_2)}$ where the operation is the exponentation of permutation groups.

The exponention of permutation groups has been defined and studied by Harary.[6] The general definition is briefly reviewed. Let $\mathcal{A}$ and $\mathcal{B}$ be permutation groups of degrees a and b operating on object sets X and Y; let the orders of $\mathcal{A}$ and $\mathcal{B}$ be m and n respectively. The exponention $\mathcal{B}^{\mathcal{A}}$ has Y^X, the class of all functions from X to Y as its object set. The elements of $\mathcal{B}^{\mathcal{A}}$ are constructed by permuting the domain X using a permutation in $\mathcal{A}$ and then permuting the image objects for every object in the domain by elements of $\mathcal{B}$. The properties of the group are summarized below in Table V.

It is interesting to note that the exponentiation of permutation groups has occurred in two combinatorial problems prior to this study. The first oc-

TABLE V

Group	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{B}^{\mathcal{A}}$
Object Set	X	Y	Y^X
Degree	a	b	b^a
Order	m	n	mn^a

currence was in Slepian's original study of the number of classes of Boolean functions.[18] The next occurrence was in Harary's study of bi-colored graphs.[7] It is interesting to note that Slepian computed $\mathcal{I}_2^{\mu_n}$ while Harary worked with $\mu_n^{\mathcal{I}_2}$. In reference 8, Slepian's original method was reformulated using the properties of the exponentiation of the two groups.

It is immediately verified that $\mathcal{A}_n(Z_2) = \mathcal{I}_2^{GL_n(Z_2)}$. The equation

$$f(\underset{\sim}{x}\, A \oplus \underset{\sim}{b}) = f((\underset{\sim}{x} \oplus \underset{\sim}{b}\, A^{-1})\, A)$$

(A^{-1} exists since $A \in GL_n(Z_2)$) shows that the group of translations $\mathcal{I}_2^n$ is a normal subgroup of $\mathcal{A}_n(Z_2)$. Thus $\mathcal{A}_n = \mathcal{I}_2^n\,(GL_n(Z_2))$.* Many algebraic identities may be derived about the relation of elements in $\mathcal{I}_2^n$ and in $GL_n(Z_2)$ but we shall not do so here. We know from references 2 and 8 that the cycle index of $\mathcal{I}_2^n$ is given by

$$Z_{\mathcal{I}_2^n} = \frac{1}{2^n}\left(f_1^{2^n} + (2^n - 1)\, f_2^{2^{n-1}}\right)$$

*By the product $\mathcal{A}\mathcal{B}$ of two groups $\mathcal{A}$ and $\mathcal{B}$ which are subgroups of a larger group $\mathcal{G}$ we mean the group whose domain is $\{ab \mid a \in \mathcal{A},\ b \in \mathcal{B}\}$. This group is defined when one of $\mathcal{A}$ or $\mathcal{B}$ is normal in $\mathcal{G}$. In our case $\mathcal{I}_2^n$ is normal in $\mathcal{A}_n(Z_2)$ and $\mathcal{A}_n(Z_2)$ is the least group containing $\mathcal{I}_2^n$ and $GL_n(Z_2)$.

The importance of this result is that there are only two types of cycle structure induced by elements of Σ_2^n. The first corresponds to the identity. When this permutation is composed with elements of $GL_n(Z_2)$, we obtain just the elements of $GL_n(Z_2)$. We must now determine the effect of multiplying a non-identity permutation in Σ_2^n with the permutations having cycle structure

$$v_{ij} = \prod_{k=1}^{j} f_1 \, f_{q_{ik}}^{h_{ik}} .$$

The answer is given in the following lemma.

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

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

Proof. Examine the v_{ij} premultiplied by the non-identity permutations of Σ_2^n.

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

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

where the sum is over all classes.

Using the polynomials constructed by this formula, the following numerical results were obtained. For $3 \leq n \leq 5$, the results agree with those of Nechiporuk.[14] 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.

TABLE VI

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

TABLE VII

	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

The following results are suggested by Table VII. $N_n^0 = N_n^1 = N_n^2 = 1$. 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 $\mathcal{L}_n$ of linear Boolean functions is preserved under $\mathcal{A}_n(Z_2)$ and that there are 3 classes of linear functions for all n.

$$[\overline{xy},\ \overline{x}y,\ x\overline{y},\ xy]\ [\overline{x} + \overline{y},\ \overline{x} + y,\ x + \overline{y},\ x + y]$$

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

4. THE NUMBER OF CLASSES WHEN THE RANGE IS COMPLEMENTED

The definition of equivalence of Boolean functions is often enlarged by also allowing complementation of the range of the functions. This subject was investigated in reference 9 and the following theorem was proved.

Theorem 4. Let $\mathcal{G}$ be any permutation group on the domain of Boolean functions. The number of classes of functions under $\mathcal{N} \times \mathcal{G}$ (transformations of $\mathcal{G}$ on the domain and complementation of the range) is given by

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

We shall apply this theorem to $GL_n(Z_2)$ and $\mathcal{A}_n(Z_2)$.

Theorem 5. The number of classes under $\mathcal{N} \times GL_n(Z_2)$ is one half the number of classes under $GL_n(Z_2)$.

Proof. Since every linear transformation in $GL_n(Z_2)$ leaves the origin invariant, every term of the cycle index has a factor f_1^k where $k \geq 1$.

The calculations for both groups are given below in Table VIII.

TABLE VIII

THE NUMBER OF CLASSES UNDER THE ENLARGED GROUPS

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

It was also shown in reference 9 that the number of self complementary classes (classes closed under complementation) under a group $\mathcal{G}$ is $Z_{\mathcal{G}}(0,2,0,2,\ldots,0,2)$. The number of such classes is given in Table IX below

TABLE IX

THE NUMBER OF SELF-COMPLEMENTARY CLASSES

n	$GL_n(Z_2)$	$\mathcal{M}_n(Z_2)$
1	0	1
2	0	1
3	0	2
4	0	4
5	0	30
6	0	7,679

One might inquire whether most of the classes of neutral functions (those with 2^{n-1} atoms in their normal form expansion) are self complementary or not

under $\mathcal{N}_n(Z_2)$. In order to obtain the 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 6. The number of neutral classes under $\mathcal{N}_n(Z_2)$ 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[12] 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 $Z_{\mathcal{G}}(0,2,\ldots,0,2)$ is $\frac{2^{2^{n-1}}}{g}$ An upper bound is certainly

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

The ratio we desire can now be computed, but it is convenient to have an estimate for the binomial coefficient. Using Stirling's formula, we get

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

The ratio of self-complementary classes to neutral class under $\mathcal{N}_n(Z_2)$ 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.

5. INVERTIBLE BOOLEAN FUNCTIONS

C. S. Lorens[12] has studied the invertible Boolean functions and has counted the number of classes of such functions with the same group acting on both the domain and range of the functions. This writer[10] has extended Lorens' results by allowing different groups on the domain and range. We now apply the techniques of reference 10 to counting the number of classes of invertible functions when $GL_n(Z_2)$ and $\mathcal{A}_n(Z_2)$ are considered.

The notation for the other groups to be studied are as follows. Γ_2^n denotes the group of all 2^n complementations of variables; the cycle index of this group was first computed by Ashenhurst.[2] $\mathcal{M}_n$ denotes the symmetric group of degree n on the variables. This group was studied by Hellerman[11] and the cycle index was first computed in reference 8. $\mathcal{J}_n$ is the least group containing Γ_2^n and $\mathcal{M}_n$. The cycle index was first computed by Pólya[16] for $1 \leq n \leq 4$. Slepian[17] first gave an algorithm for counting the number of classes under $\mathcal{J}_n$ for all n although he did not explicitly construct the cycle index. A closed form for the cycle index is given in reference 8.

Theorem 7. The number of classes of invertible functions with a group $\mathcal{G}$ acting on the domain and a group $\mathcal{H}$ acting on the range is

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

evaluated at $z_1 = z_2 = \ldots = z_s = 0$ where $Z_{\mathcal{G}}$ denotes the cycle index of $\mathcal{G}$.

Table X gives the number of classes with the same group on both the domain and range. Table XI gives the results with different groups on the domain and range. It is trivial to show that the number of classes of invertible functions with $\mathcal{L}_2^n$ on the domain and $GL_n(Z_2)$ on the range is

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

TABLE X

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

n	$\mathcal{L}_2^{n*}$	$\mathcal{M}_n^*$	$\mathcal{G}_n^*$	$GL_n(Z_2)$	$\mathcal{A}_n(Z_2)$
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

*These numbers are quoted from reference 10.

TABLE XI

n	Σ_2^n on domain $GL_n(Z_2)$ on range	$\mathcal{M}_n$ 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	Σ_2^n on domain $\mathcal{A}_n(Z_2)$ on range	$\mathcal{M}_n$ on domain $\mathcal{A}_n(Z_2)$ on range	$\mathcal{A}_n$ on domain $\mathcal{A}_n(Z_2)$ on range	$GL_n(Z_2)$ on domain $\mathcal{A}_n(Z_2)$ 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

6. ENGINEERING IMPLICATIONS

The orders of $GL_n(Z_2)$ and $\mathcal{A}_n(Z_2)$ are much larger than the other groups which have been studied previously in switching theory. Because the orders are so large, we find a smaller number of classes. This opens up the possibility of using ennumeration techniques for n = 5 or perhaps n = 6 if a computer is used. There are still several problems to be solved before the practical design methods may be developed. These problems are mentioned in detail in the next section.

The small number of classes gives some justification for the linear approach to switching circuits. It appears that the number of $\oplus$ operations which are required to realize the transformation which maps one function into an equivalent function is very small. A more precise conjecture is made in the next section.

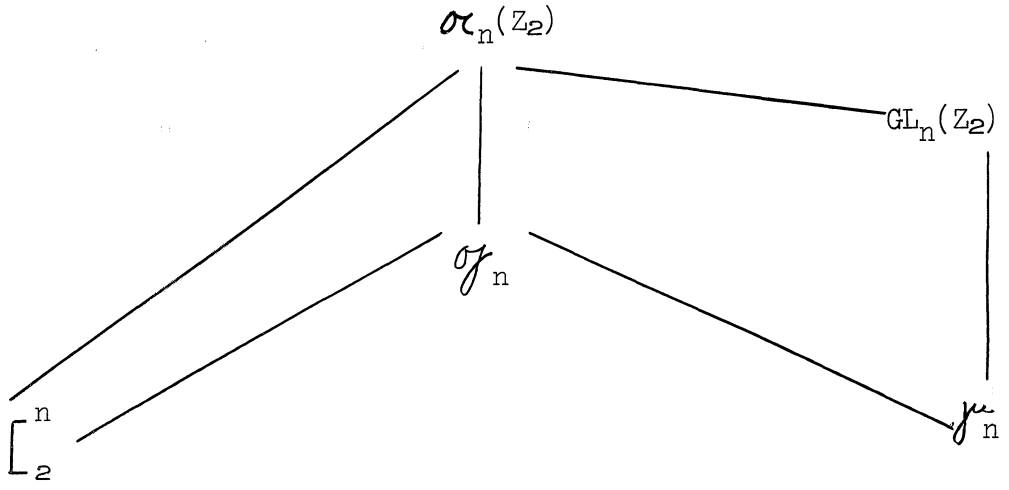
The development of cheap and fast components for realizing the $\oplus$ operation also makes this approach look more promising. Recently tunnel diode circuits for realizing the $\oplus$ operation have been reported by Menger[13] and others; these circuits require only one tunnel diode for realizing $x_1 \oplus x_2 \oplus x_3$.

7. MISCELLANEOUS COMMENTS AND PROBLEMS

The initial investigation into equivalence of Boolean functions under linear groups has been very promising, but a great many problems remain open.

The most serious unsolved problem is to find an algorithm for determining when two functions are equivalent under the groups. Nechiporuk[14] and Slepian[18] list partial results but the general problem has not been solved. A canonical form for functions under $GL_n(Z_2)$ would have applications in coding theory also.

It is a general principle that if $\mathcal{G}$ and $\mathcal{H}$ are two groups such that $\mathcal{H} \subseteq \mathcal{G}$, then the set of invariants of $\mathcal{H}$ contains the set of invariants of $\mathcal{G}$. One would like to have the invariants of $\mathcal{A}_n(Z_2)$ and all its subgroups. $\mathcal{A}_n(Z_2)$ contains all the other groups which have been studied as transformation groups on Boolean functions as subgroups. The lattice structure of these subgroups is shown below



It appears that the transformation which maps one equivalent function into another requires very few $\oplus$ operations in its hardware realization. One may also observe that the representatives of the equivalence classes are very simple for the first few values of n. It was even thought that there might be a linearly separable function in each class, but this can be shown to be false by a cardinality argument. Both of these observations about the small number of $\oplus$ operations and the simplicity of the representatives cannot be true for all n because of complexity considerations. This writer conjectures that the former observation is correct. More precisely that the number of $\oplus$ operations required to realize the transformation from $f(\underset{\sim}{x})$ to $f(\underset{\sim}{x}\ A)$, $A \in GL_n(Z_2)$ is linear in n.

The techniques given for counting the number of classes under $\mathcal{OT}_n(Z_2)$ may be immediately applied to counting the number of equivalence classes of (n,k) codes under the affine group.

8. ACKNOWLEDGMENT

I wish to thank B. Elspas who first suggested these problems and who was able to verify the results for $1 \leq n \leq 3$ under $GL_n(Z_2)$. I am indebted to C. S. Lorens for pointing out the work of Nechiporuk. Robert Lechner is also working on these and related problems and has also constructed algorithms for counting the number of classes under $GL_n(Z_2)$ and $\mathcal{OT}_n(Z_2)$. I am indebted to him for verifying my results for $1 \leq n \leq 6$ under both groups.

REFERENCES

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. Church, R., "Tables of irreducible polynomials for the first four prime moduli," Annals of Mathematics, Vo. 36, No. 1, January (1935), pp. 198-209.

4. Dickson, L. E., Linear Groups with an Exposition of the Galois Field Theory, Dover Publications, New York (1958).

5. Elspas, B., "Autonomous linear sequential networks," I.R.E. Transactions, CT-6, March (1959), pp. 45-60.

6. Harary, F., "Exponentiation of permutation groups," American Mathematical Monthly, Vol. 66, No. 7, August-September, (1959).

7. Harary, F., "On the number of bi-colored graphs," Pacific Journal of Mathematics, Vol. 8, No. 4, (1958), pp. 743-755.

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

9. Harrison, M. A., The Number of Equivalence Classes of Boolean Functions under Groups Containing Negation, The University of Michigan Technical Note 04879-4-T, June (1962).

10. Harrison, M. A., The Number of Classes of Invertible Boolean Functions, The University of Michigan Technical Note 04879-5-T, July (1962).

11. Hellerman, L., Equivalence Classes of Logical Functions, IBM Technical Publication TR00. 819, November (1961).

12. Lorens, C. S., Invertible Boolean Functions, Space General Corporation Report, July 1, (1962).

13. Menger, K. S., "A modulo two adder for three inputs using a single tunnel diode," I.R.E. Transaction, Vol. 10, No. 3, September (1961), pp. 530-531.

14. 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.

15. Pólya, G., "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen," Acta Mathematica, Vol. 68 (1937), pp. 145-253.

16. Pólya, G., "Sur les types des propositions composées," Journal of Symbolic Logic, Vol. 5 (1940), pp. 98-103.

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

18. Slepian, D., "Some further theory of group codes," The Bell System Technical Journal, Vol. XXXIX, No. 5, September (1960), pp. 1219-1252.