THE UNIVERSITY OF MICHIGAN
COLLEGE OF ENGINEERING
Department of Electrical Engineering
Information Systems Laboratory

Technical Note

THE NUMBER OF EQUIVALENCE CLASSES OF BOOLEAN FUNCTIONS UNDER GROUPS CONTAINING NEGATION

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 1962

SUMMARY

In my recent paper on combinatorial analysis,[4] algorithms were constructed for counting the number of transitivity sets of Boolean functions under three groups. The results of this previous paper will be assumed; we shall enlarge the groups under consideration by allowing complementation of functions as well as the other group operations. Algorithms are obtained for counting the number of equivalence classes under the enlarged groups. The results are applied to simplify a recent result of Elspas.[2]

The duality group is defined, and the number of classes is shown to be the same as with the negation group except in one case.

I. INTRODUCTION

In this paper, we extend the results obtained in reference 4 to the case where negation of Boolean functions is also allowed. The negation of a Boolean function is obtained by the action of a negation group to be denoted by $\mathfrak{N}$. $\mathfrak{N}$ has order two; one element is the identity mapping and the other element denoted by η has the property:

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

for any Boolean function f.

The groups to be considered are $\mathfrak{N} \times \Sigma_2^n$, $\mathfrak{N} \times \mathfrak{A}_n$, and $\mathfrak{N} \times \mathfrak{G}_n$. One can trivially show that if $\mathfrak{G}$ is any permutation group on the atoms of the free Boolean algebra, then the (abstract) structure of the group $\mathfrak{G}$ enlarged by allowing complementation of functions is $\mathfrak{N} \times \mathfrak{G}$ where the cross indicates the direct product.

Our results will be obtained by applying a special case of a theorem by De Bruijn.[1] De Bruijn's paper states that this theorem is a generalization of Pólya's famous theorem, but Harary has informed this writer (oral communication) that De Bruijn's theorem would follow from Pólya's if one could find $Z_{\mathfrak{B}^{\mathfrak{A}}}$ in terms of $Z_{\mathfrak{A}}$ and $Z_{\mathfrak{B}}$. Unfortunately the latter result is not yet known. Cf. Harrison[4] for an example of exponentiation of permutation groups.

II. DE BRUIJN'S THEOREM

For our purposes we shall need a form of De Bruijn's theorem 2.[1] The result to be used is an extremely weak consequence of this general theorem.

Let D be a finite set of d elements and R a finite set of r elements. Consider the class of functions from D to R. Let $\mathfrak{G}$ and $\mathfrak{h}$ denote permutation groups acting on D and R respectively. Two functions f_1 and f_2 are said to be equivalent if and only if there exist elements $\alpha \in \mathfrak{G}$, $\beta \in \mathfrak{h}$ such that $f_1(d) = \beta\, f_2(\alpha(d))$ for $d \in D$. Since this is a genuine equivalence relation, the family of functions is decomposed into equivalence classes. $\mathfrak{F}$ denotes the set of all such classes and F will denote an equivalence class of functions from D into R.

Before stating De Bruijn's theorem, we briefly review the concept of the cycle index polynomial (Zyklenzieger) of a permutation group $\mathfrak{G}$ whose order is g and whose degree is s. 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 $\mathfrak{G}$ 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 we define

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

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

We can now state our simplified form of De Bruijn's theorem.

Theorem 1. (De Bruijn) *If we let*

$$h_t = \exp\left\{t \sum_{k=1}^{\infty} z_{kt}\right\} \qquad \text{for } t = 1,\ldots,r$$

then

$$\sum_{F \in \mathfrak{F}} 1 = Z_{\mathcal{G}}\left(\frac{\partial}{\partial z_1},\ldots,\frac{\partial}{\partial z_s}\right) Z_{\mathfrak{h}}(h_1,\ldots,h_r)$$

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

Thus the counting problem is solved once we know both cycle indices. It is to be understood that the variables in these polynomials are indeterminates. Therefore we can differentiate formally and no questions of existence or convergence ever arise.

Lemma 2. *A term* $h_1^{j_1} \ldots h_r^{j_r}$ *in* $Z_{\mathfrak{h}}$ *gives rise to*

$$Z_{\mathcal{G}}\left(\sum_{t|1} tj_t, \ldots, \sum_{t|s} tj_t\right)$$

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

This yields

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

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

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

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

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

Taking all the z's equal to zero gives

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

III. APPLICATIONS

We now specialize our approach to handle an arbitrary permutation group $\mathcal{G}$ of degree 2^n and order g. For Boolean functions $D = \{0,1\}^n$ so $d = 2^n$ and $R = \{0,1\}$. If $\mathcal{H}$ is taken to be the negation group $\mathcal{N}$, then we note that the action of the negation group is to permute the elements of the range of the Boolean functions. So $\mathcal{N}$ is really the symmetric group of degree (and order) two; hence

$$Z_{\mathcal{N}} = \frac{1}{2} (h_1^2 + h_2)$$

Using De Bruijn's theorem and the lemma gives

Theorem 3. <u>If $\mathcal{G}$ is any permutation group on the 2^n min-terms, then the number of equivalence classes of Boolean functions under $\mathcal{N} \times \mathcal{G}$ is</u>

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

We note that $Z_{\mathcal{G}} (2,2,\ldots,2)$ is the total number of classes of functions under the group $\mathcal{G}$. Since it is necessary to construct $Z_{\mathcal{G}}$ in order to count the classes under $\mathfrak{G}$, we see that no additional work is required to count the number of classes under $\mathfrak{N} \times \mathfrak{G}$.

We list the number of classes under $\mathfrak{N} \times \Sigma_2^n$, $\mathfrak{N} \times \mathfrak{S}_n$, and $\mathfrak{N} \times \mathfrak{G}_n$. The cycle indices for these groups were constructed in reference 4. The pertinent results are listed here without proof.

Theorem 4.

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

$$Z_{\mathfrak{S}_n} = \frac{1}{n!} \sum_{(j)} \frac{n!}{1^{j_1} j_1! \ldots n^{j_n} j_n!} \mathop{\times}_{i=1}^{n} \left(\prod_{d \mid i} f_d^{e(d)} \right)^{j_i}$$

$$Z_{\mathfrak{G}_n} = \frac{1}{n! 2^n} \sum_{(j)} \frac{n!}{1^{j_1} j_1! \ldots n^{j_n} j_n!} \mathop{\times}_{i=1}^{n} \left(\prod_{d \mid i} f_d^{e(d)} + \prod_{\substack{d \nmid i \\ d \mid 2i}} f_d^{g(d)} \right)^{j_i}$$

where the last two indices are summed over all partitions of n such that $\sum_{i=1}^{n} i j_i = n$. The functions (x), e, and g are defined in reference 4.

Σ_2^n is the group of complementations of variables; $\mathfrak{S}_n$ is the group of permutations of variables. $\mathfrak{G}_n$ is the group of complementations and permutations of variables. It is shown in reference 4 that $\mathfrak{G}_n = \mathfrak{S}^n_{\Sigma_2}$. The group $\mathfrak{N} \times \mathfrak{G}_n$ has already been studied by Golomb[3] who did not, however, count the number of classes.

Since an explicit formula has been obtained for $Z_{\Sigma_2^n}$, we get the following result.

Theorem 5. <u>The number of classes under</u> $\mathfrak{N} \times \mathfrak{C}_2^n$ <u>is</u>

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

Theorem 6. <u>The number of classes under</u> $\mathfrak{N} \times \mathfrak{S}_n$ <u>is</u>

$$\frac{1}{2} Z_{\mathfrak{S}_n} (2,\ldots,2)$$

<u>i.e., half the number of classes under</u> $\mathfrak{S}_n$.

The rest of the results are tabulated below.

Number of Classes Under Groups Without Complementation of Functions

n	$\mathfrak{C}_2^n$	$\mathfrak{S}_n$	$\mathfrak{G}_n$
1	3	4	3
2	7	12	6
3	46	80	22
4	4,336	3,984	402
5	134,281,216	37,333,248	1,228,158
6	288,230,380,379,570,176	25,626,412,338,274,304	400,507,806,843,728

Number of Classes Under Groups With Complementation of Functions

n	$\mathfrak{C}_2^n$	$\mathfrak{S}_n$	$\mathfrak{G}_n$
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	114,115,192,303,714,304	12,813,206,169,137,152	200,253,952,527,184

We may apply theorem 1 to obtain some information about groups without negation of functions. If $\mathcal{H}$ is taken to be just the identity alone, then the total number of equivalence classes under $\mathcal{G}$ is $Z_{\mathcal{G}}(2,\ldots,2)$. Comparing this to theorem 3, we get the following result.

Theorem 7. *The number of classes of functions under $\mathcal{G}$ which are equivalent to their complements, i.e., self-complementary, is*

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

We compute the following numbers:

Number of Classes of Self-Complementary Functions

n	Σ_2^n	$\mathcal{M}_n$	$\mathcal{G}_n$
1	1	0	1
2	3	0	2
3	14	0	6
4	240	0	42
5	63,488	0	4,094
6	4,227,858,432	0	98,210,640

The results in the last column (for $n \leqslant 5$) were obtained independently by Elspas[2] by a laborious method. It is easy to show that no function is equivalent to its negation under $\mathcal{M}_n$ directly. For Σ_2^n, the number of self-complementary classes is $(2^n - 1)2^{2^{n-1}-n}$.

IV. THE DUALITY GROUP

We can define a group $\mathcal{D}$ having order two whose non-trivial element δ

has the property

$$\delta: f(x_1,\ldots,x_n) \longrightarrow f^D(x_1,\ldots,x_n) = \bar{f}(\bar{x}_1,\ldots,\bar{x}_n)$$

for any Boolean function f. One would naturally ask about the number of classes under say $\mathcal{D} \times \Sigma_2^n$ and $\mathcal{D} \times \mathcal{G}_n$. In these cases it is easy to prove that we get the same number of classes as with $\mathcal{N} \times \Sigma_2^n$ and $\mathcal{N} \times \mathcal{G}_n$, by constructing a one-to-one mapping between the classes under the different groups. The case of $\mathcal{D} \times \mathcal{A}_n$ is somewhat special; the discussion of this group is postponed until the sequel.

Recently Toda[5] has counted the number of classes under $\mathcal{G}_n$ which consist of only self-dual functions. It is interesting to observe that Toda's results do not give the number of classes closed under the duality operation; this latter number is somewhat larger, namely $Z_{\mathcal{G}_n}(0,2,0,2,\ldots,0,2)$. This result may be seen by showing that the equivalence classes of the two groups are the same.

n	Number of Classes Under $\mathcal{D} \times \mathcal{G}_n$	Number of Classes of Self-Dual Functions Under $\mathcal{G}_n$*	Number of Classes Under $\mathcal{G}_n$ Closed Under the Duality Operation
1	2	1	1
2	4	1	2
3	14	3	6
4	222	7	42
5	616,126	83	4,094
6	200,253,952,527,184	109,958	98,210,640

*These results are quoted from Toda's paper.[5]

REFERENCES

1. N. G. De Bruijn, "Generalization of Pólya's fundamental theorem in enumerative combinatorial analysis," Koninklijke Nederlandse Akademie Van Wetenschappen, Series A, Vol. LXII, No. 2 (1959), pp. 56-59.

2. B. Elspas, "Self-complementary symmetry types of Boolean functions," IRE Transactions of Electronic Computers, Vol. EC-9, No. 2 (1960), pp. 264-266.

3. S. Golomb, "On the classification of Boolean functions," IRE Transactions on Information Theory, Vol. IT-5 (1959), pp. 176-186.

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

5. I. Toda, "On the number of types of self-dual logical functions," IRE Transactions on Electronic Computers, Vol. EC-11, No. 2 (1962).