PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 100(114) (2016), 95–99 DOI: 10.2298/PIM1614095C

ON THE NUMBER OF EQUIVALENCE CLASSES OF INVERTIBLE BOOLEAN FUNCTIONS UNDER ACTION OF PERMUTATION OF VARIABLES ON DOMAIN AND RANGE

Marko Carić and Miodrag Živković

ABSTRACT. Let V_n be the number of equivalence classes of invertible maps from $\{0,1\}^n$ to $\{0,1\}^n$, under action of permutation of variables on domain and range. So far, the values V_n have been known for $n \leqslant 6$. This paper describes the procedure by which the values of V_n are calculated for $n \leqslant 30$.

1. Introduction

Let V_n be the number of equivalence classes of invertible maps from $\{0,1\}^n$ to $\{0,1\}^n$, under action of permutation of variables on domain and range. Lorens [**1**] gave a method for calculating the number of equivalence classes of invertible Boolean functions under the following group operations on the input and output variables: complementation, permutation, composition of complementation and permutation, linear transformations and affine transformations. In particular, he calculated the values V_n for $n \leqslant 5$. Irvine [**4**] in 2011 calculated V_6 (the sequence A000653). In this paper using a more efficient procedure, the values V_n are calculated for $n \leqslant 30$.

2. Notation

Let S_r denote symmetric group on r letters. Consider a set of vectorial invertible Boolean functions (hereinafter referred to as functions), i.e., the set S_N of permutations of $B_n = \{0,1\}^n$ where $N = 2^n$. The function $F \in S_N$ maps the n-tuple $X = (x_1,\dots,x_n) \in B_n$ into $Y = (y_1,\dots,y_n) = F(X)$. For some permutation $\sigma \in S_n$, the result of its action on $X = (x_1,\dots,x_n) \in B_n$ is $\sigma'(X) = (x_{\sigma(1)},\dots,x_{\sigma(n)}) \in B_n$.

An arbitrary pair $(\rho,\sigma) \in S_n^2$ determines mapping $T_{\rho,\sigma} : S_N \to S_N$, defined by $T_{\rho,\sigma}(F) = \rho' \circ F \circ \sigma'$ where $F \in S_N$; in other words, if $F' = T_{\rho,\sigma}(F)$ then

2010 *Mathematics Subject Classification:* Primary 05A15; Secondary 06E30.
Key words and phrases: invertible Boolean functions, number of equivalence classes, permutation group.
Communicated by Žarko Mijajlović.

$F'(X) = \rho'(F(\sigma'(X)))$ for all $X \in B_n$. The set of all mappings $T_{\rho,\sigma}$ with respect to composition is a subgroup of $S_{N!}$.

The two functions $F, H \in S_N$ are considered equivalent if there exist permutations $\rho, \sigma \in S_n$ such that $H = T_{\rho,\sigma}(F)$, i.e., if they differ only by a permutation of input or output variables.

Let ι denote the identity permutation. Every permutation $\sigma \in S_n$ uniquely determines the permutation $\sigma' \in S_N$. Let S'_n denote the subgroup of S_N consisting of all permutations σ' corresponding to permutations $\sigma \in S_n$. The mapping $\sigma \mapsto \sigma'$ is a monomorphism from S_n to S_N (see [**2**]).

Let $\sigma \in S_r$. Let p_i, $1 \leqslant i \leqslant r$, denote the number of cycles of length i in a cycle decomposition of σ; here $\sum_{i=1}^{r} ip_i = r$. The cycle index monomial of σ is the product $\prod_{i=1}^{r} t_i^{p_i}$ where t_i, $1 \leqslant i \leqslant r$, are independent variables. It can be equivalently described by the vector $\operatorname{spec}(\sigma) = p = (p_1, p_2, \dots, p_r)$. For an arbitrary positive integer n let $P_n = \{(p_1, p_2, \dots, p_n) \mid p_i \geqslant 0, \sum_{i=1}^{n} ip_i = n\}$ denote the set of partitions of n. For some $p \in P_n$ let $S_{n,p} = \{\sigma \in S_n \mid \operatorname{spec}(\sigma) = p\}$. An arbitrary partition p corresponds to the decomposition $n = k_{p,1} + k_{p,2} + \cdots + k_{p,m(p)}$ into positive summands $k_{p,1} \geqslant k_{p,2} \geqslant \cdots \geqslant k_{p,m(p)} > 0$ where summand $i = n, n-1, \dots, 1$ in this sum appears p_i times.

Let $\langle r, s\rangle$ and (r, s) denote the least common multiple and the greatest common divisor of r and s, respectively.

3. Preliminaries

The calculation of V_n is based on the following known facts (see e.g., [**1**–**3**]):

(1) The cardinality of $S_{n,p}$ equals to

$$|S_{n,p}| = \frac{n!}{\prod_i i^{p_i} p_i!}.$$

(2) Let $\sigma_1, \sigma_2 \in S_n$ be permutations such that $\operatorname{spec}(\sigma_1) = \operatorname{spec}(\sigma_2)$. Then $\operatorname{spec}(\sigma'_1) = \operatorname{spec}(\sigma'_2)$. In other words, permutations with the same cycle index in S_n induce the permutations with the same cycle index in S'_n.

(3) The permutation $T_{\rho,\sigma}$ has at least one fixed point if and only if $\operatorname{spec}(\sigma) = \operatorname{spec}(\rho)$.

(4) Let $\sigma \in S_{n,p}$ and let $\operatorname{spec}(\sigma') = p' = (p'_1, p'_2, \dots, p'_N)$. The number of fixed points of $T_{\sigma,\sigma}$ is

$$N_p = \prod_i i^{p'_i} p'_i!.$$

(5) If $\sigma \in S_n$ is a cyclic permutation (a permutation having only one cycle of the length n), then the cycle index monomial of the permutation σ' is

$$\prod_{d|n} f_d^{e(d)},$$

where the numbers $e(k), k \geqslant 1$ are defined by the recurrent relation

$$e(k) = \frac{1}{k}\Big(2^k - \sum_{d|k, d<k} d \cdot e(d)\Big), \quad k > 1.$$

with the initial value $e(1) = 2$.

(6) If α is a permutation on a set X with $|X| = a$ and α has a cycle index monomial $f_1^{j_1} \cdots f_a^{j_a}$, and β is a permutation on Y with $|Y| = b$ and β has a cycle index monomial $f_1^{k_1} \cdots f_b^{k_b}$, then the permutation (α, β) acting on $X \times Y$ by the rule

$$(\alpha, \beta)(x, y) = (\alpha(x), \beta(y))$$

has cycle index monomial given by

$$\Big(\prod_{p=1}^{a} f_p^{j_p}\Big) \bigtimes \Big(\prod_{q=1}^{b} f_q^{k_q}\Big) = \prod_{p=1}^{a}\prod_{q=1}^{b}(f_p^{j_p} \times f_q^{k_q}) = \prod_{p=1}^{a}\prod_{q=1}^{b} f_{\langle p,q\rangle}^{j_p k_q (p,q)}.$$

4. The number of equivalence classes

The value of V_n is determined by the following theorem.

Theorem 4.1. *For an arbitrary $p \in P_n$ let $\sigma \in S_{n,p}$. If* $\operatorname{spec}(\sigma') = (p'_1, \ldots, p'_n)$, *then*

$$V_n = \sum_{p \in P_n} \frac{\prod_i i^{p'_i} p'_i!}{\big(\prod_i i^{p_i} p_i!\big)^2}. \tag{4.1}$$

Proof. The permutation $F \in S_N$ is a fixed point of $T_{\rho,\sigma}$ if $T_{\rho,\sigma}(F(X)) = F(X)$ holds for all $X \in B_n$. Let $I(\rho, \sigma)$ be a number of fixed points of $T_{\rho,\sigma}$. By the Frobenius lemma (see e.g. [**1**]) the number of equivalence classes is equal to

$$V_n = \frac{1}{(n!)^2} \sum_{\sigma \in S_n} \sum_{\rho \in S_n} I(\rho, \sigma) = \frac{1}{(n!)^2} \sum_{p \in P_n} \sum_{\rho \in S_{n,p}} \sum_{q \in P_n} \sum_{\sigma \in S_{n,q}} I(\rho, \sigma).$$

By the facts (2)–(4) from Preliminaries, the number of fixed points of $T_{\rho,\sigma}$ corresponding to fixed permutations $\rho \in S_{n,p}$, $\sigma \in S_{n,q}$ is equal to

$$I(\rho, \sigma) = \begin{cases} 0, & p \neq q \\ N_p, & p = q \end{cases}$$

Therefore

$$\begin{aligned} V_n &= \frac{1}{(n!)^2} \sum_{p \in P_n} \sum_{\rho \in S_{n,p}} \sum_{q \in \{p\}} \sum_{\sigma \in S_{n,p}} N_p = \frac{1}{(n!)^2} \sum_{p \in P_n} \sum_{\rho \in S_{n,p}} \sum_{\sigma \in S_{n,p}} N_p \\ &= \frac{1}{(n!)^2} \sum_{p \in P_n} N_p \sum_{\rho \in S_{n,p}} \sum_{\sigma \in S_{n,p}} 1 = \frac{1}{(n!)^2} \sum_{p \in P_n} N_p \cdot |S_{n,p}|^2 \\ &= \sum_{p \in P_n} \frac{\prod_i i^{p'_i} p'_i!}{\big(\prod_i i^{p_i} p_i!\big)^2}. \end{aligned}$$

$\square$

By induction the following generalization of the fact (6) can be proved. If α_i is permutation on Z_i, $|Z_i| = k_i$, $i = 1, \ldots, n$, and if the cycle index monomial of α_i is $f_1^{y_{i,1}} \cdots f_{k_i}^{y_{i,k_i}}$, then the permutation $(\alpha_1, \ldots, \alpha_n)$ acting on $Z_1 \times Z_2 \times \cdots \times Z_n$ by the rule

$$(\alpha_1, \ldots, \alpha_n)(z_1, \ldots, z_n) = (\alpha_1(z_1), \ldots, \alpha_n(z_n))$$

has cycle index monomial given by

$$\begin{aligned} \bigtimes_{i=1}^{n} \left(\prod_{z_i=1}^{k_i} f_{z_i}^{y_{i,z_i}} \right) &= \prod_{z_1=1}^{k_1} \prod_{z_2=1}^{k_2} \cdots \prod_{z_n=1}^{k_n} \bigtimes_{i=1}^{n} f_{z_i}^{y_{i,z_i}} \\ &= \prod_{z_1=1}^{k_1} \prod_{z_2=1}^{k_2} \cdots \prod_{z_n=1}^{k_n} f_{\langle z_1, z_2, \ldots, z_n \rangle}^{\prod_{i=1}^{n} (z_i y_{i,z_i})/\langle z_1, z_2, \ldots, z_n \rangle} \end{aligned} \tag{4.2}$$

The proof is based on the fact, also proved by induction, that the cycle index monomial of the direct product of n permutations with cycle index monomials $f_{z_i}^{y_i}$, $1 \leqslant i \leqslant n$ is equal to

$$\bigtimes_{i=1}^{n} f_{z_i}^{y_i} = f_{\langle z_1, z_2, \ldots, z_n \rangle}^{\prod_{i=1}^{n} (z_i y_i)/\langle z_1, z_2, \ldots, z_n \rangle}$$

Using this generalization, the following theorem shows how to obtain the cycle index p' of σ', used in previous theorem.

THEOREM 4.2. *Let $p \in P_n$ be an arbitrary partition and let $\sigma \in S_{n,p}$. Let $\sigma = \alpha_1 \alpha_2 \ldots \alpha_m$ be a decomposition of σ into disjoint cycles. Let the length of α_i be k_i, $1 \leqslant i \leqslant m$. The cycle index monomial $\prod_i f_i^{p'_i}$ of the corresponding σ' is given by*

$$\bigtimes_{i=1}^{m} \left(\prod_{z_i | k_i} f_{z_i}^{e(z_i)} \right) = \prod_{z_1 | k_1} \prod_{z_2 | k_2} \cdots \prod_{z_m | k_m} f_{\langle z_1, z_2, \ldots, z_m \rangle}^{\prod_{i=1}^{m} z_i e(z_i)/\langle z_1, z_2, \ldots, z_m \rangle} \equiv \prod_i f_i^{p'_i}.$$

PROOF. The cycle of length k_i in σ induces the product of cycles in σ' with the cycle index monomial $\prod_{z_i | k_i} f_{z_i}^{e(z_i)}$. The product of permutations with cycle index monomial $\prod_{i=1}^{n} t_i^{p_i} = \prod_{i=1}^{m} t_{k_i}$ in σ induces a permutation with the cycle index monomial $\bigtimes_{i=1}^{m} \prod_{z_i | k_i} f_{z_i}^{e(z_i)}$ in σ'. The cycle index of σ' is then obtained using (4.2)

$$\prod_i f_i^{p'_i} = \prod_{z_1 | k_1} \prod_{z_2 | k_2} \cdots \prod_{z_m | k_m} f_{\langle z_1, z_2, \ldots, z_m \rangle}^{\prod_{i=1}^{m} z_i e(z_i)/\langle z_1, z_2, \ldots, z_m \rangle}. \qquad \square$$

The following diagram displays the dependence of the computation time on n. More precisely, the natural logarithms of the two times (in seconds), denoted by T_n and T'_n, respectively, are displayed—the time needed to compute V_n, and the time needed to compute only cycle indexes of $\sigma \in S_{n,p}$ and σ' for all partitions $p \in P_n$. It is seen that the most time-consuming part of the algorithm is the calculation including large numbers.

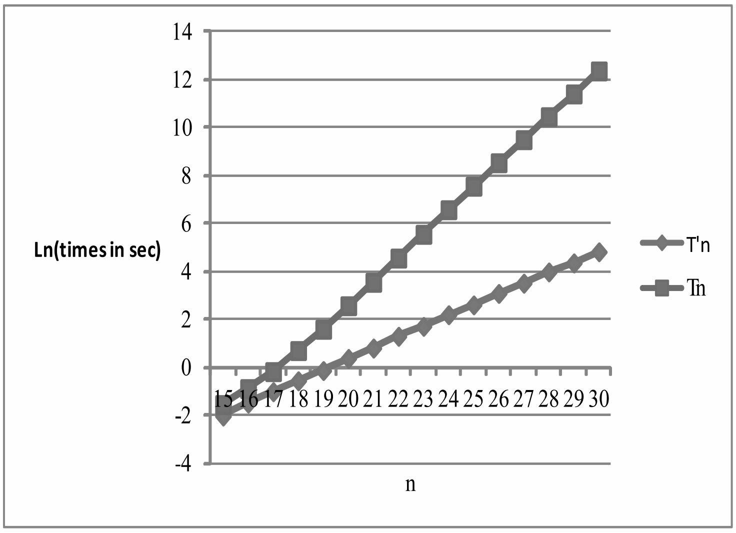

FIGURE 1. Computation time.

5. Acknowledgement

We are greatly indebted to the anonymous referee for many useful comments.

References

1. C. S. Lorens, *Invertible Boolean functions*, IEEE Trans. Electron. Comput. **EC-13** (1964), 529–541.
2. M. A. Harrison, *The number of transitivity sets of boolean functions*, J. Soc. Ind. Appl. Math. **11**(3) (1963), 806–828.
3. M. A. Harrison, *Counting theorems and their applications to switching theory*, Chapter 4 in A. Mukhopadyay (ed.), *Recent Developments in Switching Functions*, Academic Press, New York, 1971, 85–120.
4. *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://oeis.org, 2010.

Advanced School of Electrical Engineering Applied Studies
Belgrade
Serbia
caric.marko@gmail.com

(Received 06 01 2016)
(Revised 03 02 2016 and 23 04 2016)

Faculty of Mathematics
Department of Informatics
University of Belgrade
Serbia
ezivkovm@matf.bg.ac.rs