Research Article

Thomas W. Cusick*, K. V. Lakshmy and M. Sethumadhavan

Affine equivalence of monomial rotation symmetric Boolean functions: A Pólya's theorem approach

DOI: 10.1515/jmc-2016-0042
Received March 9, 2016; accepted September 30, 2016

Abstract: Two Boolean functions are affine equivalent if one can be obtained from the other by applying an affine transformation to the input variables. For a long time, there have been efforts to investigate the affine equivalence of Boolean functions. Due to the complexity of the general problem, only affine equivalence under certain groups of permutations is usually considered. Boolean functions which are invariant under the action of cyclic rotation of the input variables are known as rotation symmetric (RS) Boolean functions. Due to their speed of computation and the prospect of being good cryptographic Boolean functions, this class of Boolean functions has received a lot of attention from cryptographic researchers. In this paper, we study affine equivalence for the simplest rotation symmetric Boolean functions, called MRS functions, which are generated by the cyclic permutations of a single monomial. Using Pólya's enumeration theorem, we compute the number of equivalence classes, under certain large groups of permutations, for these MRS functions in any number n of variables. If n is prime, we obtain the number of equivalence classes under the group of all permutations of the variables.

Keywords: Affine equivalence, rotation symmetry, Boolean functions, Pólya's counting theorem

MSC 2010: 94C10, 94A60, 06E30

Communicated by: Otokar Grosek

1 Introduction

The subject of Boolean functions is well established and constitutes a cornerstone of cryptography and coding theory. Let $\mathbb{F}_2$ be the binary finite field and $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A Boolean function on n variables may be viewed as a mapping from $\mathbb{F}_2^n \to \mathbb{F}_2$. The set of all n-variable Boolean functions is denoted by $\mathscr{B}_n$. Functions which are invariant under the action of the cyclic group are called rotation symmetric functions. These functions were first introduced by Pieprzyk and Qu in 1999 [19] and used as components in hashing algorithms to speed up the implementation of a cryptographic hash function. Since then, rotation symmetric Boolean functions have proven to be very useful in several areas of cryptography [3, 9, 10, 14, 19, 22]. These functions are extremely rich in terms of cryptographically significant functions. A Boolean function is said to be monomial rotation symmetric (MRS) if it is generated by the cyclic permutations of the variables in a single monomial.

The problem of enumerating the types of Boolean functions under the group of variable permutations and complementation was first stated by Jevons in the 1870s, but not solved in a satisfactory way until the

***Corresponding author: Thomas W. Cusick:** Mathematics Department, University at Buffalo, Buffalo, NY 14260, USA, e-mail: cusick@buffalo.edu
K. V. Lakshmy, M. Sethumadhavan: TIFAC CORE in Cyber Security, Amrita School of Engineering, Coimbatore Amrita Vishwa Vidyapeetham, Amrita University, India, e-mail: lakshmyviswanathan@gmail.com, m_sethu@cb.amrita.edu

work of Pólya [20] in 1937. An affine transformation provides a method of grouping similar Boolean functions into classes. It is meaningful for the following two reasons: first, equivalent functions have similar properties like Hamming weight distribution and same nonlinearity; second, the number of representatives is much less than the number of Boolean functions. Two functions $f, g \in \mathscr{B}_n$ are said to be affine equivalent if there exist a nonsingular $n \times n$ matrix A over $\mathbb{F}_2$ and a vector $b \in \mathbb{F}_2^n$ such that $g(x) = f(Ax \oplus b)$. We say that $f(Ax \oplus b)$ is a *nonsingular affine transformation* of $f(x)$. The first notable effort to solve an affine equivalence problem is found in a 1964 paper of Harrison [12]. In 1972 Berlekamp and Welch [1] identified and described the complete set of equivalence classes for functions of five inputs using their algebraic normal form. In 1991, Maiorana [17] computed 150,357 equivalence classes of six variable Boolean functions. Due to its complexity and size, affine equivalence still remains a tough problem to deal with, especially for a general solution, which addresses any $n \in \mathbb{N}$. In 2009 Kim, Park and Hahn [15] studied the affine equivalence of the quadratic MRS Boolean functions. Cusick [4] found the affine equivalence classes in certain cases for the cubic MRS functions by introducing a new concept called patterns. An exact formula for the number of classes was given in the case where the number of variables n is a prime. In 2014, Cusick and Cheon [6] extended the work of [4] to the quartic MRS Boolean functions, including an exact formula for n prime. In 2015 Stănică [23] used ideas from the theory of circulant matrices to give a new proof of the results of [6] and also obtained an exact formula for the case where n is a prime power. Recently Cusick and Stănică [8] derived an asymptotic formula for the number $A_{d,p}$ of affine equivalence classes under *all* permutations for degree d MRS Boolean functions where the number of variables p is prime, namely

$$A_{d,p} = \frac{1}{d!}p^{d-2} + \frac{1}{d!}\frac{d^2 - d - 2}{2}p^{d-3} + \mathcal{O}(p^{d-4}) \quad \text{if } d \geq 5.$$

They also gave an exact formula for the quintic MRS functions when n is a prime power. Still the enumeration of affine equivalence of MRS Boolean functions of degree d for an arbitrary number of variables was unanswered.

We solve a special case of this problem of enumeration of affine equivalence of MRS Boolean functions using Pólya's theory. We define a certain permutation group, the action of which on the set of monomials in n variables gives the affine equivalence of MRS Boolean functions under that permutation group.

The rest of the paper is organized as follows: In Section 2, we provide basic definitions and notations. In Section 3, we state Pólya's enumeration theorem for the sake of completeness. In Section 4, we explain the results that we need for the study of affine equivalence. In Section 5, we prove the theorems which give the counts of the equivalence classes for monomial rotation symmetric Boolean functions under some groups of permutations. This section contains the main results in this paper. In Section 6, we discuss some possibilities for future work and finally, in Section 7, we summarize the paper.

2 Preliminaries

A Boolean function on n variables may be viewed as a mapping from $\mathbb{F}_2^n \to \mathbb{F}_2$ and can be represented as a multivariate polynomial over $\mathbb{F}_2$, that is

$$f(x_1, x_2, \ldots, x_n) = \sum_{j=(j_1,j_2,\ldots,j_n)\in \mathrm{GF}(2)^n} a_j x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n},$$

where $a_j \in \mathbb{F}_2$ and the addition and multiplication are over $\mathbb{F}_2$. This representation is called the algebraic normal form (ANF). The algebraic degree of f is defined as the maximum number of variables in the terms in the ANF of f. If all the terms in the ANF of f have the same degree then the function is said to be homogeneous.

Definition 2.1 (Cyclic rotation). Given variables x_i, for any $2 \leq i \leq n$ and $0 \leq k \leq n-1$ we define

$$\rho_n^k(x_i) = \begin{cases} x_{i+k} & \text{if } i + k \leq n, \\ x_{i+k-n} & \text{if } i + k > n. \end{cases}$$

Let $x = (x_1, x_2, \dots, x_n) \in F_2^n$. Then we can extend the definition of ρ_n^k to tuples and monomials as follows:

$$\rho_n^k(x) = (\rho_n^k(x_1), \rho_n^k(x_2), \dots, \rho_n^k(x_n)) \quad \text{and} \quad \rho_n^k(x_{i_1}x_{i_2}\cdots) = \rho_n^k(x_{i_1})\rho_n^k(x_{i_2})\dots.$$

Definition 2.2 (Rotation symmetric Boolean function). A Boolean function f is called rotation symmetric if, for each input $(x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$,

$$f(\rho_n^1(x_1, x_2, \dots, x_n)) = f(x_1, x_2, \dots, x_n).$$

Note that the rotation symmetric Boolean function f possesses the same value for each of the subsets generated from the rotational symmetry. The inputs of a rotation symmetric Boolean function can be divided into orbits so that each orbit consists of all cyclic shifts of one input. An orbit generated by $(x_1, x_2, \dots, x_n)$ is

$$O_n(x_1, x_2, \dots, x_n) = \{\rho_n^k(x_1, x_2, \dots, x_n) \mid 0 \le k < n\}$$

and the function has the same value for all inputs in the same orbit. Let g_n be the number of such orbits. Then the number of rotation symmetric Boolean functions is 2^{g_n}. Note that if the ANF of the rotation symmetric function contains a term $x_{i_1}x_{i_2}\cdots x_{i_d}$, then, by the definition of rotation symmetry, it has all the terms from the orbit

$$O_n(x_{i_1}x_{i_2}\cdots x_{i_d}) = \{\rho_n^k(x_{i_1}x_{i_2}\cdots x_{i_d}) \text{ for } 0 \le k < n\}$$

of $x_{i_1}x_{i_2}\cdots x_{i_d}$.

Definition 2.3 (SANF). The representation of the rotation symmetric Boolean function f as

$$f = a_0 + a_1x_1 + \sum_j a_{1j}x_1x_j + \dots + a_{12\cdots n}x_1x_2\cdots x_n,$$

where $a_0, a_1, \dots, a_{12\cdots n} \in \mathbb{F}_2$, and the existence of a representative term $x_1x_{i_2}\cdots x_{i_l}$ imply the existence of all terms from $O_n(x_1x_{i_2}\cdots x_{i_l})$ in the ANF is called the simplified ANF (SANF).

Definition 2.4 (MRS Boolean function). A rotation symmetric Boolean function f is said to be monomial rotation symmetric (MRS) if the SANF of f contains only one term. In that case the function f of degree d has the form

$$f(x) = x_1x_{i_2}x_{i_3}\cdots x_{i_d} + x_2x_{i_2+1}x_{i_3+1}\cdots x_{i_d+1} + \dots + x_nx_{i_2-1}x_{i_3-1}\cdots x_{i_d-1}.$$

Definition 2.5 (Permutation preserving rotation symmetry). We say that a permutation σ of the n variables preserves rotation symmetry if for any given rotation symmetric Boolean function f in n variables the function $\sigma(f)$ is also rotation symmetric.

The results in [4] and [6] give a method for explicitly determining the equivalence classes under permutations which preserve rotation symmetry for any cubic or quartic MRS function in n variables, and also give an exact formula for the number of classes if n is a prime. In the cubic case, the equivalence classes under permutations which preserve rotation symmetry when n is prime are the same as the equivalence classes under all permutations. This was first proved in [5, Theorem 3], and then was generalized to the case of functions (of any degree) where n is any prime in [8]. The corresponding result is certainly not true for composite n, because already for quartic MRS functions with $n = 8$ there is an example [6, Remark 1.10] where there are five equivalence classes under all permutations, but six if only permutations which preserve rotation symmetry are considered. It is known [8, Theorem 2.3] that the group of permutations preserving rotation symmetry when the number of variables is a prime p has order $p - 1$. In this paper we consider equivalence classes for MRS functions in n variables under a group (defined below) of permutations of order $n\phi(n)$, and it turns out that for prime n the equivalence classes under this group are the same as the classes for the group of permutations which preserve rotation symmetry, and so are the same as the classes under all permutations.

3 Pólya's enumeration theorem

Some of the most difficult problems in mathematics involve counting. There are several reasons for this difficulty, some of which are technical and others more conceptual. A frequently encountered technical difficulty is that the objects to be counted may not be sequentially arranged. A common conceptual difficulty occurs when different objects are identified for enumeration purposes. The problem then is to enumerate equivalence classes. Two main theorems in combinatorics concerned with counting mathematical objects with regards to symmetry are Burnside's lemma and Pólya's enumeration theorem [20]. Pólya's enumeration theorem, also known as Redfield–Pólya's theorem (because of the work in [21]), is a powerful generalization of Burnside's lemma which takes symmetry into account when counting mathematical objects. Burnside's lemma, while powerful in its own right, can require a significant amount of computation. Pólya's enumeration theorem minimizes the computations needed by the use of the cycle index and explores the idea of weights which enables the pursuit of more complex problems.

Lemma 3.1 (Burnside's lemma). *Let G be a group of permutations acting on a set X. Then the number of distinct orbits, which we call patterns, induced on X under the action of G is given by*

$$\frac{1}{|G|}\sum_{\sigma\in G}|\mathrm{Inv}(\sigma)|, \quad \textit{where}\ \mathrm{Inv}(\sigma)=\{x\in X \mid \sigma(x)=x\}.$$

In order to compute the number of patterns using Burnside's lemma we must first compute the size of $Inv(\sigma)$ for all $\sigma \in G$. Pólya observed that elements of G with the same cycle structure made the same contribution to the sets of fixed points. He defined the notion of cycle index polynomial (or, for brevity, cycle index) to keep track of the cycle structure of the elements of G.

Definition 3.1 (Cycle index polynomial). Let G be a permutation group on n symbols. For $\sigma \in G$ let $l_k(\sigma)$ denote the number of cycles of σ of length k. Then the cycle index polynomial of G is a polynomial in n variables $x_1, x_2, \dots, x_n$ given by

$$Z_G(x_1,x_2,\dots,x_n)=\frac{1}{|G|}\sum_{\sigma\in G}\prod_{i=1}^{n}x_i^{l_i(\sigma)}.$$

Let G_1, G_2 be permutation groups acting on sets X_1, X_2 respectively. Let $G = G_1 \times G_2$ be the direct product of groups and $X = X_1 \times X_2$ the cartesian product of corresponding sets. For an element $x = (x_1, x_2)$ of X and an element $g = (g_1, g_2)$ of G, we define the action of g on x by

$$\phi(g,x)=(\phi_1(x_1,g_1),\phi_2(x_2,g_2)).$$

Harary [11, p. 746] introduced a combinatorial multiplication of polynomials (we use the notation $\circledast$) to find the cycle index polynomial of the product group $G_1 \times G_2$ in terms of the cycle index polynomial of the groups G_1 and G_2. Let

$$Z_{G_1}(f_1,f_2,\dots,f_l)=\sum_{(j)}c_{(j)}\prod_{p=1}^{l}f_p^{j_p},\quad Z_{G_2}(f_1,f_2,\dots,f_m)=\sum_{(k)}d_{(k)}\prod_{q=1}^{m}f_q^{k_q}.$$

Then

$$Z_{G_1}\circledast Z_{G_2}=\sum_{(j)}c_{(j)}\sum_{(k)}d_{(k)}\prod_{p=1}^{l}f_p^{j_p}\circledast\prod_{q=1}^{m}f_q^{k_q},$$

where the $\circledast$ operation on the indeterminates is defined as

$$\prod_{p=1}^{l}f_p^{j_p}\circledast\prod_{q=1}^{m}f_q^{k_q}=\prod_{p=1}^{l}\prod_{q=1}^{m}f_p^{j_p}\circledast f_q^{k_q}$$

and

$$f_p^{j_p}\circledast f_q^{k_q}=f_{\mathrm{lcm}(p,q)}^{j_pk_q\gcd(p,q)}.$$

Lemma 3.2. *Let the cycle index polynomial of the action of the group G_1 on the set X_1 be $Z_{(G_1,X_1)}$ and of G_2 on X_2 be $Z_{(G_2,X_2)}$. Then the cycle index of the natural action of the permutation group $G_1 \times G_2$ on $X_1 \times X_2$ induced by actions G_1 on X_1 and G_2 on X_2 can be expressed as*

$$Z_{(G_1\times G_2, X_1\times X_2)} = Z_{(G_1,X_1)} \circledast Z_{(G_2,X_2)}.$$

Proof. This lemma seems to have been first proved by Harary [11, pp. 745–746] in 1958. □

We note that some applications of this lemma have previously been given by Harrison [13].

Now we explain the version of Pólya's theorem that we shall use. Let X be a set. A coloring of X is an assignment of a color to each element of X. That is, a coloring corresponds to a function $f : X \to C$, where C is a set of colors. When $|X| = k$ and $|C| = m$, there are m^k colorings of X using the colors from C. A weight function w is any function from a set C of colors into the set X. Given a set of colors C we want to assign a weight w_c for all $c \in C$; then we define the weight of a coloring to be the product of the weights of the colored elements. In this paper X will be the set of all monomials of a given degree d in n variables, with weighted colorings as explained in the next paragraph, and the action of a group G of permutations will induce an equivalence relation on X. The equivalence classes will be the patterns in Pólya's theorem (see Lemma 3.1 and the discussion of counting the patterns which follows the lemma) and the cycle index will be the generating function for the number of equivalence classes, as explained in Theorem 5.2 below. A thorough exposition of our version of Pólya's theorem (with weights) is given in [2].

In our context of MRS Boolean functions in n variables, the color set will be $C = \{0, 1\}$ and the associated two weights will be $w_0 = 1$ and $w_1 = y$. Given any monomial in n variables, we color a variable x_i, $1 \le i \le n$, with color 1 if x_i does not appear in the monomial and with color y if x_i does appear in the monomial. Thus the weight of any monomial of degree d is always y^d and by rotation symmetry all the monomials in any MRS function in n variables will have the same weight.

Theorem 3.3 (Pólya's enumeration theorem). *If a group G acts on a set X whose elements are colored by elements of C, which are weighted by w, then the expression*

$$Z_G\Big(\sum_{i=1}^{m} w_{c_i}, \sum_{i=1}^{m} w_{c_i}^2, \dots, \sum_{i=1}^{m} w_{c_i}^n\Big)$$

generates the pattern inventory of distinct colorings by weight, where $Z_G(x_1, x_2, \dots, x_n)$ is the cycle index polynomial of G.

4 Affine equivalence of MRS Boolean functions

Definition 4.1 (Affine equivalence). Two functions $f, g \in \mathscr{B}_n$ are said to be affine equivalent if there exist a nonsingular $n \times n$ matrix A over $\mathbb{F}_2$ and a vector $b \in \mathbb{F}_2^n$ such that $g(x) = f(Ax \oplus b)$. We say that $f(Ax \oplus b)$ is a *nonsingular affine transformation* of $f(x)$.

The simplest nonsingular affine transformations of an MRS function f are obtained if we simply permute the n variables, in which case A is a permutation matrix and $b = \mathbf{0}$. At present it seems too difficult to handle affine equivalence in general, so we will only consider equivalence under permutations, or under subgroups of the group of all permutations, in this paper. If σ is a permutation of the n variables, we have $\sigma(f) = f(Ax)$, where A is the permutation matrix which permutes the subscripts of the variables in accordance with σ. Notice that such a permutation of the variables does not necessarily preserve rotation symmetry. If we have $\sigma(f) = f(Ax) = g$ for some MRS function g, then we say that f and g are *permutation equivalent*.

Affine equivalence is a useful notion in cryptography because many cryptographically relevant properties of a Boolean function f are preserved under affine equivalence, and so are said to be *affine invariants*. For example, it is easy to see that the Hamming weight (notation wt(f)) and nonlinearity (notation nl(f)) (for definitions, see for example [7, pp. 6–7]) of a Boolean function are affine invariants. For two quadratic functions

$f, g \in \mathscr{B}_n$ we have the well-known stronger result that f and g are affine equivalent if and only if $\mathrm{wt}(f) = \mathrm{wt}(g)$ and $\mathrm{nl}(f) = \mathrm{nl}(g)$, but this is not true for functions of higher degree. It is also known [4, Theorem 2.7] that if two quadratic MRS functions in $\mathscr{B}_n$ are affine equivalent, then they are permutation equivalent. Thus in the quadratic case there is no loss of generality in only considering equivalence under permutations, but again this is not true for higher degrees.

To begin our study of the permutation equivalence of MRS Boolean functions of degree d we define a group G_n of permutations. Let $g_{\tau j}$ be a permutation on $\mathbb{Z}_n$ defined by (we omit the dependence on n from the notation, since it will be clear from the context whenever we use it)

$$g_{\tau j}(i) = (i + j - 1)\tau + 1 \pmod{n}, \tag{4.1}$$

where the notation $a \,(\mathrm{mod}\, n)$ means the unique integer b in $\{1, 2, \dots, n\}$ such that $b \equiv a \,(\mathrm{mod}\, n)$. Let $G_n = \{g_{\tau j} : \gcd(\tau, n) = 1 \text{ and } 1 \le j \le n\}$. Then G_n forms a group of order $n\phi(n)$ under the operation of permutation composition. Let X be the set of all monomials of degree d in n variables. Define the action of G_n on X as follows:

$$g_{\tau j}(x_{i_1} x_{i_2} \cdots x_{i_d}) = x_{g_{\tau j}(i_1)} x_{g_{\tau j}(i_2)} \cdots x_{g_{\tau j}(i_d)}. \tag{4.2}$$

We give some examples of the groups G_n below. We use the notation e for the identity and give other permutations as a product of cycles, with fixed points omitted.

Examples of the groups G_n

The group G_{10} has 4 elements $g_{\tau 1}$ with $\tau \in \{1, 3, 7, 9\}$, namely e and

$$(1, 4, 3, 10)(2, 7)(5, 6, 9, 8),\ (1, 8, 7, 10)(2, 5, 6, 3)(4, 9),\ (1, 10)(2, 9)(3, 8)(4, 7)(5, 6).$$

The other 36 elements $g_{\tau j}$ with $j > 1$ are derived from these by (4.1).

The group G_{15} has 8 elements $g_{\tau 1}$ with $\tau \in \{1, 2, 4, 7, 8, 11, 13, 14\}$, namely e and

$$\begin{gathered}(1, 3, 7, 15)(2, 5, 11, 8)(4, 9)(6, 13, 12, 10),\ (1, 5, 6, 10, 11, 15)(2, 9, 7, 14, 12, 4)(3, 13, 8),\\ (1, 8, 12, 10, 11, 3, 7, 5, 6, 13, 2, 15)(4, 14, 9),\ (1, 9, 13, 15)(3, 10, 6, 4)(5, 11, 14, 8)(7, 12),\\ (1, 12, 13, 9, 10, 6, 7, 3, 4, 15)(2, 8, 14, 5, 11),\ (1, 14, 3, 10, 11, 9, 13, 5, 6, 4, 8, 15)(2, 12, 7),\\ (1, 15)(2, 14)(3, 13)(4, 12)(5, 11)(6, 10)(7, 9).\end{gathered}$$

The other 112 elements $g_{\tau j}$ with $j > 1$ are derived from these by (4.1).

We define

$$M_{d,n} = \{\text{all MRS functions of degree } d \text{ in } n \text{ variables}\}.$$

It seems that we must also consider the set

$$F_{d,n} = \{M_{d,n} \text{ plus functions generated by the action of } G_n \text{ on } M_{d,n}\},$$

but in fact we show in our next lemma that this set is the same as $M_{d,n}$.

Lemma 4.1. *For any given n all of the permutations in the group G_n preserve rotation symmetry, so we have $F_{d,n} = M_{d,n}$ for all degrees d.*

Proof. It suffices to consider only the $\phi(n)$ elements $g_{\tau 1}$ in G_n, since for any fixed τ with $\gcd(\tau, n) = 1$ each permutation $g_{\tau j}$ with fixed j satisfies $g_{\tau j}(i) = g_{\tau 1}(i + j - 1)$, $1 \le i \le n$. Thus if the set of monomials in an MRS function is preserved by the action of $g_{\tau 1}$, then it is also preserved by the action of any $g_{\tau j}$, $1 \le i \le n$.

Now consider the action of $g_{\tau 1}$ on the monomials in the MRS function f generated by the monomial $x_{i_1} x_{i_2} \cdots x_{i_d}$. The images of these monomials are the monomials

$$x_{i_1\tau+1+\tau k} x_{i_2\tau+1+\tau k} \cdots x_{i_d\tau+1+\tau k}, \quad 1 \le k \le n. \tag{4.3}$$

By elementary number theory, $\{\tau k \mid 1 \le k \le n\} = \{1, 2, \dots, n\}$ when $\gcd(\tau, n) = 1$, so the monomials in (4.3) are the monomials in some MRS function which is equivalent to f. Thus $g_{\tau 1}$ preserves rotation symmetry. □

Our proofs below require the use of another group H_n, defined as follows: Let n be a positive integer and let $\sigma_{t,s}$ be a permutation on $\mathbb{Z}_n$ defined by

$$\sigma_{t,s}(i) = it + s \pmod{n}.$$

Let

$$H_n = \{\sigma_{t,s} : \gcd(t, n) = 1 \text{ and } 0 \le t,\ s \le n - 1\}.$$

Then H_n forms a group of order $n\phi(n)$ under the operation of permutation composition. As before, let X be the set of all monomials of degree d in n variables. Define the action of H_n on X as follows:

$$\sigma_{t,s}(x_{i_1} x_{i_2} \cdots x_{i_k}) = x_{\sigma_{t,s}(i_1)} x_{\sigma_{t,s}(i_2)} \cdots x_{\sigma_{t,s}(i_k)}.$$

Wei and Xu [24, pp. 180–181] have found the cycle index polynomial for this group H_n by using the following lemma (we corrected several typographical errors in [24]).

Lemma 4.2. *Let p be an odd prime and $\alpha \ge 1$. Then the cycle index of $Z_{H_{p^\alpha}}$ is*

$$\begin{aligned} Z_{H_{p^\alpha}}(x_1, x_2, \ldots, x_{p^\alpha}) = \frac{1}{p^{2\alpha-1}(p-1)} \Big\{ & \sum_{w=1}^{\alpha} p^{2(w-1)}(p-1) x_{p^w}^{p^{\alpha-w}} \\ & + \sum_{w=0}^{\alpha-1} \sum_{t \mid p-1} p^{w+\delta(t)(\alpha-w)} \phi(tp^w) x_1 x_t^{\frac{p^{\alpha-w-1}-1}{t}} \times \Big(\prod_{u=0}^{w} x_{tp^u}\Big)^{\frac{p^{\alpha-w-1}(p-1)}{t}} \Big\}, \end{aligned}$$

where

$$\delta(t) = \begin{cases} 1 & \text{if } t > 1, \\ 0 & \text{if } t = 1. \end{cases}$$

The cycle index of H_{2^α} is

$$Z_{H_{2^\alpha}}(x_1, x_2, \ldots, x_{2^\alpha}) = \begin{cases} \frac{1}{2}(x_1^2 + x_2) & \text{if } \alpha = 1, \\ \frac{1}{8}(x_1^4 + 2x_1^2 x_2 + 3x_2^2 + 2x_4) & \text{if } \alpha = 2, \\ \frac{1}{2^{2\alpha-1}} \Big\{ 2^{2\alpha-3} x_{2^\alpha} + \sum_{w=1}^{\alpha-1} (2^{2(w-1)} + \phi(2^{w-1}) 2^{\alpha-1}) x_{2^w}^{2^{\alpha-w}} & \\ \quad + \sum_{w=0}^{\alpha-2} \phi(2^w)(2^w x_1^{2^{\alpha-w}} + 2^{\alpha-1} x_1^2 x_2^{2^{\alpha-w-1}-1}) \times \Big(\prod_{u=1}^{w} x_{2^u}\Big)^{2^{\alpha-w-1}} \Big\} & \text{if } \alpha \ge 3. \end{cases}$$

Given Lemma 4.2, we can find the cycle index polynomial Z_{H_n} for any n by using the multiplication $\circledast$ from Section 3 and Lemma 3.2. This was done in [24], whose authors were apparently unaware of the much earlier work, mentioned in Section 3, involving the $\circledast$ operation.

We need the group H_n because it turns out that the cycle index polynomials Z_{G_n} and Z_{H_n} are the same. We were unable to compute Z_{G_n} directly. It is easy to see that the groups G_n and H_n are isomorphic, but this does not suffice to show that they have the same cycle index polynomials. We prove this in our next lemma.

Lemma 4.3. *For all integers $n > 1$ the groups G_n and H_n have the same cycle index polynomial.*

Proof. From the definition of the permutations $g_{\tau,j}$ and $\sigma_{t,s}$, for any τ with $\gcd(\tau, n) = 1$ we have the equality of functions

$$g_{\tau,j} = \sigma_{\tau,\tau(j-1)+1}.$$

For any i, $1 \le i \le n$, we have

$$\sigma_{t,s}(i) = (i + st^{-1} + 1 - t^{-1} - 1)t + 1 = g_{t,st^{-1}+1-t^{-1}}(i),$$

hence this isomorphism preserves the cycle structure also. Therefore the cycle index polynomial of G_n is the same as the cycle index polynomial of H_n. □

5 Permutation equivalence of MRS functions

This section contains the core results in this paper. Our next theorem applies the machinery developed in Section 4 to the MRS functions.

Theorem 5.1. *The group G_n acts on the set $M_{d,n}$ by* (4.2) *and the orbits are the equivalence classes for $M_{d,n}$ under the group G_n. If n is a prime p, then the equivalence classes from the action* (4.2) *of G_p are the same as the equivalence classes for $M_{d,p}$ under all permutations of the variables.*

Proof. The first sentence of the theorem follows from the definitions. For the second sentence, we observe that the group G_p contains the group of order $p-1$ defined in [8], whose group action orbits are the equivalence classes for $M_{d,p}$. But by [8, Theorem 2.1] these equivalence classes are the same as the classes under all permutations when n is prime, and of course G_p is contained in the group of all permutations. Hence the equivalence classes under G_p are the same as the equivalence classes under all permutations. □

We note that Theorem 5.1 for prime values of n was previously proved by Cusick and Stănică [8].

We shall apply Pólya's Theorem 3.3 to the action of G_n on $M_{d,n}$, and then will prove the following theorem.

Theorem 5.2. *Define the action of G_n on $M_{d,n}$ by applying the action of G_n defined by* (4.2) *on*

$$X = \{\text{all monomials of degree } d \text{ in } n \text{ variables}\}$$

to each of the monomials in any function in $M_{d,n}$. Let the elements of X be colored from the set of colors $\{0, 1\}$, *with weights $w_0 = 1$ and $w_1 = y$. We assign color* 0 *and weight w_0 to any variable x_i which does not appear in a given monomial, and we assign color* 1 *and weight w_1 to any variable which does appear. Let $Z_{G_n}(x_1, x_2, \ldots, x_n)$ be the cycle index polynomial. Then the coefficient of y^d in the pattern inventory*

$$Z_{G_n}(1+y, 1+y^2, \ldots, 1+y^n)$$

is the number of affine equivalence classes for $M_{d,n}$ under the group G_n. We can compute all of these coefficients explicitly, provided we can compute the factors of n and of $p-1$ for every prime p which divides n.

Proof. We use Pólya's Theorem 3.3 with $G = G_n$, the given action of G_n on $M_{d,n}$, and the given colors and weights. Then by Theorem 5.1 the orbits are the orbits for $M_{d,n}$. Of course the weight of a monomial is the product of the weights of its variables. Thus the weight of a monomial is y^d, where d is the degree of the corresponding MRS function, so by Theorem 3.3 the number of equivalence classes $E_{d,n}$ is the coefficient of y^d in the pattern inventory $Z_{G_n}(1+y, 1+y^2, \ldots, 1+y^n)$. By Lemma 4.3 we can use Z_{H_n} instead of Z_{G_n}, and by the formulas in Lemmas 4.2 and 3.2 we can explicitly compute the number of equivalence classes, provided we can compute the factors of n and of $p-1$ for every prime p which divides n. This proves the theorem. □

Let $E_{d,n}$ denote the number of affine equivalence classes for $M_{d,n}$ under the group G_n. Then Theorem 5.2 states that

$$E_{d,n} = \text{coefficient of } y^d \text{ in } Z_{G_n}(1+y, 1+y^2, \ldots, 1+y^n). \tag{5.1}$$

We give an explicit evaluation for the formula (5.1) when n is an odd prime in our next theorem.

Theorem 5.3. *When n is an odd prime p, the number of equivalence classes of MRS Boolean functions of degree d in p variables under the group of all permutations is*

$$E_{d,p} = \frac{1}{p(p-1)}\left[\binom{p}{d} + p \sum_{\substack{t \mid \gcd(p-1,d) \\ t>1}} \phi(t) \binom{\frac{p-1}{t}}{\frac{d}{t}} + p \sum_{\substack{t \mid \gcd(p-1,d-1) \\ t>1}} \phi(t) \binom{\frac{p-1}{t}}{\frac{d-1}{t}}\right]. \tag{5.2}$$

Proof. By Theorem 5.1 it is enough to count the equivalence classes for $M_{d,p}$ under the group G_p. We will use Pólya's Theorem 3.3 to count the equivalence classes, using the method explained in Theorem 5.2, with $n = p$. Theorem 5.2 says that $E_{d,p}$ is the coefficient of y^d in

$$Z_{G_p}(1+y, 1+y^2, \ldots, 1+y^p),$$

and by Theorem 4.3 we can replace G_p with the group H_p. Now the special case $\alpha = 1$ of Theorem 4.2 gives

$$Z_{H_p}(x_1, x_2, \dots, x_p) = \frac{1}{p(p-1)}\Big[x_1^p + (p-1)x_p + p \sum_{\substack{t|(p-1)\\ t>1}} \phi(t) x_1 x_t^{\frac{(p-1)}{t}}\Big].$$

Finally, evaluating

$$Z_{H_p}(1 + y, 1 + y^2, \dots, 1 + y^p)$$

and extracting the coefficient of y^d gives (5.2). □

As an illustration of the usefulness of Theorem 5.3, the reader can easily recover the formula $E_{3,p} = [p/6] + 1$ for cubic MRS functions [4, Theorem 4.2] by evaluating $E_{3,p}$ using (5.2). The evaluation of $E_{d,n}$ rapidly increases in complexity as the number of prime factors of n increases, but it is easy to write a computer program for these calculations. The authors have such a program using the SAGE software to quickly evaluate $E_{d,n}$ for $d < 10$ and n with up to a total of about six prime factors, counted with multiplicity.

Let $c_{d,n}$ denote the number of MRS Boolean functions of degree d in n variables; then from [16] we have

$$c_{d,n} = \frac{1}{n} \sum_{t|\gcd(d,n)} \phi(t) \binom{\frac{n}{t}}{\frac{d}{t}}. \tag{5.3}$$

Combining this with Theorem 5.3, we get the next theorem.

Theorem 5.4. *For any odd prime p and any degree d, we can define $E_{d,p}$ recursively by*

$$E_{d,p} = c_{d,p-1} + c_{d-1,p-1} - c_{d,p}.$$

Proof. Substituting (5.3) into (5.2), we get the recursion in the theorem. □

It would be interesting to find a proof of Theorem 5.4 which does not use Theorem 5.3.

If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, then by Lemma 3.2 the cycle index of G_n is given by

$$Z_{G_n}(x_1, x_2, \dots, x_n) = \circledast_{i=1}^{s} Z_{G_{p_i^{\alpha_i}}}. \tag{5.4}$$

If E_{G_n} denotes the polynomial

$$Z_{G_n}(1 + y, 1 + y^2, \dots, 1 + y^n),$$

then by (5.1) the coefficient of y^d is $E_{d,n}$. So we can use (5.4) to compute cycle index polynomials and also the polynomials E_{G_n}. We give some examples computed with a SAGE program.

Examples of cycle index polynomials

We have

$$Z_{G_{10}} = (1/40)(x_1^{10} + 5x_1^2x_2^4 + 10x_1^2x_4^2 + 6x_2^5 + 10x_2x_4^2 + 4x_5^2 + 4x_{10})$$

and

$$\begin{aligned} Z_{G_{15}} = (1/120)(&x_1^{15} + 15x_1x_2^7 + 5x_1^3x_2^6 + 3x_1^5x_2^5 + 10x_1^3x_4^3 + 30x_1x_2x_4^3 \\ &+ 20x_3x_{12} + 10x_3x_6^2 + 2x_3^5 + 12x_5x_{10} + 4x_5^3 + 8x_{15}). \end{aligned}$$

Note that a correct formula

$$Z_{G_n} = (1/(n\phi(n))p(x_1, \dots, x_n)$$

must have the sum of the integer coefficients, say c_i, of the polynomial p equal to $n\phi(n)$, and each monomial $c_i x_{i(1)}^{a(1)} \cdots x_{i(k)}^{a(k)}$ must satisfy

$$a(1)i(1) + \dots + a(k)i(k) = n.$$

Examples of polynomials E_{G_n} and equivalence class counts $E_{d,n}$

Recall that the coefficient of x^d in $E_{G_n}(x)$ is $E_{d,n}$. We have the following results:

$$\begin{aligned}
E_{G_{10}} &= 1 + x + 3x^2 + 4x^3 + 9x^4 + 9x^5 + 9x^6 + 4x^7 + 3x^8 + x^9 + x^{10},\\
E_{G_{15}} &= 1 + x + 3x^2 + 7x^3 + 18x^4 + 34x^5 + 54x^6 + 66x^7 + 66x^8 + 54x^9\\
&\quad + 34x^{10} + 18x^{11} + 7x^{12} + 3x^{13} + x^{14} + x^{15},\\
E_{G_{24}} &= 1 + y + 7y^2 + 23y^3 + 97y^4 + 294y^5 + 870y^6 + 2051y^7 + 4272y^8 + 7352y^9\\
&\quad + 10,980y^{10} + 13,790y^{11} + 15,008y^{12} + 13,790y^{13} + 10,980y^{14} + 7352y^{15}\\
&\quad + 4272y^{16} + 2051y^{17} + 870y^{18} + 294y^{19} + 97y^{20} + 23y^{21} + 7y^{22} + y^{23} + y^{24}.
\end{aligned}$$

6 Future work

Theorems 5.2 and 5.3 give a complete description of permutation equivalence for MRS functions of any degree when the number n of variables is a prime, but for other values of n only the classes under the group G_n are obtained. It would be desirable to get more detailed information about the classes when n is composite, especially since the example for $n = 8$ in the final paragraph of Section 2 shows that the answer cannot be as simple as in the prime case. It turns out that this same issue arises in some graph theory problems [25, Section 9].

It would be interesting to know, for general n, how much larger the groups G_n or H_n could be made without decreasing the number of equivalence classes given in Theorem 5.3. To do this, a deeper knowledge of the structure of those groups might be useful. We give some information about these groups in the rest of this section.

The groups G_p and H_p for prime p have been studied for a long time (see [18] for example). We can give very explicit descriptions of the structure of the groups in this case. Let $GA(p)$ denote the well-known *general affine group* $Z_p \rtimes Z_p^*$ (semidirect product) for odd primes p. It is clear from their definitions that both G_p and H_p are isomorphic to $GA(p)$. Since

$$\sigma_{1,1}(i) = i + 1 \pmod{p} \tag{6.1}$$

gives a p-cycle and $\sigma_{k,p-1}(i)$ gives a $(p-1)$-cycle for suitably chosen k, we can prove the following lemmas about the group H_p.

Lemma 6.1. *We can represent H_p as the normalizer of the subgroup K of the symmetric group S_p generated by the p-cycle $(12 \cdots p)$.*

Proof. Since $|H_p| = p(p-1)$ and H_p contains a subgroup K of order p generated by the p-cycle

$$\mu = (12 \cdots p),$$

the other generator of H_p must be a $(p-1)$-cycle ν which normalizes K. This means

$$\nu K \nu^{-1} = K,$$

which is equivalent to

$$\nu\mu\,\nu^{-1} = \mu^{(p-1)/2}, \tag{6.2}$$

since then

$$\{\nu\mu^k\,\nu^{-1} = (\nu\mu\nu^{-1})^k : 1 \le k \le p\} = \{\mu^{k(p-1)/2} : 1 \le k \le p\} = K. \qquad \square$$

Lemma 6.2. *In the representation $H_p = \langle \mu, \nu \rangle$ in terms of the generators μ, ν we can choose*

$$\nu = \sigma_{(p-1)/2,(p+3)/2}. \tag{6.3}$$

Thus ν is a $(p-1)$-cycle with $\nu(1) = 1$ and $\nu(p-1) = 2$.

Proof. From (6.1) and (6.3) we have

$$\nu(\mu^2(i)) = \nu(i+2) = \frac{p-1}{2}i + \frac{p+1}{2} \tag{6.4}$$

and (since $\mu^{-1}(i) = i - 1 \pmod{p}$)

$$\mu^{-1}(\nu(i)) = \mu^{-1}\frac{p-1}{2}i + \frac{p+3}{2} = \frac{p-1}{2}i + \frac{p+1}{2}. \tag{6.5}$$

From (6.4) and (6.5) we obtain $\nu\mu^2 = \mu^{-1}\nu$ which is equivalent to

$$(\nu\mu\nu^{-1})^2 = \nu\mu^2\nu^{-1} = \mu^{-1} = \mu^{p-1}$$

and this implies (6.2). □

7 Conclusion

We defined a group of permutations whose action on the set of monomials gives the affine equivalence classes of MRS Boolean functions in n variables, under certain large groups of permutations. If n is prime, we obtain the classes under all permutations. Using Pólya's theorem we gave an explicit count of these classes. We also gave a recurrence relation which, for prime n, expresses the number of equivalence classes of degree d MRS Boolean functions in terms of three values of the counting function which gives the number of MRS Boolean functions of given degree, in a given number of variables.

Acknowledgment: The authors thank the reviewers for their very useful suggestions, which resulted in greatly increased clarity of the exposition in the manuscript.

References

[1] E. R. Berlekamp and L. R. Welch, Weight distributions of the cosets of the (32, 6) Reed–Muller code, *IEEE Trans. Inform. Theory* **18** (1972), 203–207.

[2] N. G. de Bruijn, Pólya's theory of counting, in: *Applied Combinatorial Mathematics*, John Wiley and Sons, New York (1964), 144–164.

[3] C. Carlet, G. Gao and W. Liu, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions, *J. Combin. Theory Ser. A* **127** (2014), 161–175.

[4] T. W. Cusick, Affine equivalence of cubic homogeneous rotation symmetric functions, *Inform. Sci.* **181** (2011), 5067–5083.

[5] T. W. Cusick, Permutation equivalence of cubic rotation symmetric functions, *Int. J. Comput. Math.* **92** (2015), 1568–1573.

[6] T. W. Cusick and Y. Cheon, Affine equivalence of quartic homogeneous rotation symmetric Boolean functions, *Inform. Sci.* **259** (2014), 192–211.

[7] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Elsevier Academic Press, Amsterdam, 2009.

[8] T. W. Cusick and P. Stănică, Counting equivalence classes for monomial rotation symmetric Boolean functions with prime dimension, *Cryptogr. Commun.* **8** (2016), 1–15.

[9] G. Gao, T. W. Cusick and W. Liu, Families of rotation symmetric functions with useful cryptographic properties, *IET Inform. Secur.* **8** (2014), 297–302.

[10] G. Gao, X. Zhang, W. Liu and C. Carlet, Constructions of quadratic and cubic rotation symmetric bent functions, *IEEE Trans. Inform. Theory* **58** (2012), 4908–4913.

[11] F. Harary, On the number of bi-colored graphs, *Pacific J. Math.* **8** (1958), 743–755.

[12] M. A. Harrison, On the classification of Boolean functions by the general linear and affine groups, *J. Soc. Industrial Appl. Math.* **12** (1964), 285–299.

[13] M. A. Harrison and R. G. High, On the cycle index of a product of permutation groups, *J. Combin. Theory* **4** (1968), 277–299.

[14] S. Kavut, Results on rotation symmetric S-boxes, *Inform. Sci.* **201** (2012), 93–113.

[15] H. Kim, S.-M. Park and S.-G. Hahn, On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2, *Discrete Appl. Math.* **157** (2009), 428–432.

[16] K. V. Lakshmy, M. Sethumadhavan and T. W. Cusick, Counting rotation symmetric functions using Pólya's theorem, *Discrete Appl. Math.* **169** (2014), 162–167.

[17] J. A. Maiorana, A classification of the cosets of the Reed-Muller code $\mathscr{R}(1,6)$, *Math. Comp.* **57** (1991), 403–414.

[18] G. A. Miller, On the holomorph of a cyclic group, *Trans. Amer. Math. Soc.* **4** (1903), 153–160.

[19] J. Pieprzyk and C. X. Qu, Fast hashing and rotation-symmetric functions, *J. UCS* **5** (1999), 20–31.

[20] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68** (1937), 145–254.

[21] J. H. Redfield, The theory of group-reduced distributions, *Amer. J. Math.* **49** (1927), 433–455.

[22] V. Rijmen, P. Barreto and D. Filho, Rotation symmetry in algebraically generated cryptographic substitution tables, *Inform. Process. Lett.* **106** (2008), 246–250.

[23] P. Stănică, Affine equivalence of quartic monomial rotation symmetric Boolean functions in prime power dimension, *Inform. Sci.* **314** (2015), 212–224.

[24] W.-D. Wei and J.-Y. Xu, Cycle index of direct product of permutation groups and number of equivalence classes of subsets of $\mathscr{Z}_v$, *Discrete Math.* **123** (1993), 179–188.

[25] D. Wiedemann and M. Zieve, Equivalence of sparse circulants: The bipartite Ádám problem, preprint (2007), https://arxiv.org/abs/0706.1567.