A CHARACTERIZATION OF k-ROTATION SYMMETRIC BOOLEAN FUNCTIONS

JOSÉ E. CALDERÓN-GÓMEZ, LUIS A. MEDINA, AND CARLOS MOLINA-SALAZAR

Abstract. Rotation symmetric Boolean functions were introduced by Pieprzyk and Qu in the late 1990's. They showed that these functions are useful, among other things, in the design of fast hashing algorithms with strong cryptographic properties. The concept of rotation symmetric Boolean functions has been generalized to a class of functions known as k-rotation Boolean functions, where k divides n and n is the number of variables of the Boolean function. Analogous to the case of regular rotation symmetric Boolean functions, a monomial k-rotation Boolean function is called long k-cycle if the number of terms coincides with n/k and short k-cycle if the number of terms is less than n/k. In this work we characterize short k-cycles by providing specific generators for them. We also provide a count of short k-cycles.

1. Introduction

Boolean functions are mathematical objects that lie in the intersection of combinatorics and number theory. These objects have applications to a variety of scientific fields, including, but not limited to, coding theory, cryptography and information theory. Formally, an n-variable Boolean function is a map from $\mathbb{F}_2^n \to \mathbb{F}_2$ where $\mathbb{F}_2$ represents the binary field. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. It is not hard to see that $|\mathcal{B}_n| = 2^{2^n}$.

Every Boolean function $f \in \mathcal{B}_n$ can be identified with a multi-variable polynomial

$$f(X_1, \ldots, X_n) = \bigoplus_{\boldsymbol{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \lambda_{\boldsymbol{a}} \prod_{j=1}^{n} X_j^{a_j}, \tag{1.1}$$

where $\lambda_{\boldsymbol{a}} \in \mathbb{F}_2$ for every $\boldsymbol{a} \in \mathbb{F}_2^n$ and $\oplus$ represents addition mod 2. This polynomial is known as the *algebraic normal form* (or ANF for short) of the Boolean function f. Since every Boolean function can be identified with a multi-variable polynomial, it is natural to consider the degree of a Boolean function. The *algebraic degree* of $f \in \mathcal{B}_n$ is the degree of its ANF.

The information of a Boolean function can be recorded in a vector known as its truth table. Order the elements of the vector space $\mathbb{F}_2^n$ in lexicographical order. Let $\mathbf{x}_0 = (0, 0, \ldots, 0, 0), \mathbf{x}_1 = (0, 0, \ldots, 0, 1), \mathbf{x}_2 = (0, 0, \ldots, 1, 0), \ldots, \mathbf{x}_{2^n-1} = (1, 1, \ldots, 1, 1)$. The *truth table* of $f \in \mathcal{B}_n$ is the vector $[f(\mathbf{x}_0), f(\mathbf{x}_1), \ldots, f(\mathbf{x}_{2^n-1})]$. The *Hamming weight* of a vector $\mathbf{x} \in \mathbb{F}_2^n$, usually denoted by $wt(\mathbf{x})$, is the number of its entries that are equal to 1. The *weight* (or Hamming weight) of a Boolean function $f \in \mathcal{B}_n$, denoted by $wt(f)$, is the number of 1's in its truth table.

A property important in some cryptographic applications is balancedness. An n-variable Boolean function $f \in \mathcal{B}_n$ is called *balanced* if the number of zeros and the number of ones in its truth table are the same. Balancedness of Boolean functions is usually studied via Hamming weights or via exponential sums. The exponential sum of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$S(f) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})}. \tag{1.2}$$

Observe that a Boolean function is balanced if and only if $S(f) = 0$. The Hamming weight of a Boolean function and its exponential sum are linked by the equation

$$wt(f) = 2^{n-1} - \frac{1}{2} S(f). \tag{1.3}$$

Other desirable properties in cryptography include (but are not limited to) non-linearity, resiliency, bentness, etc. For more comprehensive information about Boolean functions, please refer to [2, 18].

Date: March 16, 2023.

2020 *Mathematics Subject Classification.* 05E05, 11T23.

Key words and phrases. k-rotation monomial Boolean functions, short and long k-cycles.

The search of Boolean functions with good cryptographic properties is a hard problem. One reason for this is the fact that $|\mathfrak{B}_n| = 2^{2^n}$, which has the consequence of making exhaustive searches over $\mathfrak{B}_n$ not feasible even for small values of n. Another problem is that the calculation of properties like the balancedness of a Boolean function using the definition of transformations like the exponential sum is analogous to using its truth table. In both cases we must perform 2^n calculations in order to obtain the answer. Because of these problems, scientists often impose conditions on the underlying Boolean functions in order to ease these difficulties. One way to do this is to study Boolean functions that are invariant under the action of certain finite groups. If G is the group acting on $\mathcal{B}_n$, then we call the Boolean functions invariant under this action *G-invariant Boolean functions*. Two of the most well-known families of these type of functions are symmetric Boolean functions and rotation symmetric Boolean functions. Their balancedness as well as other cryptographic attributes have been the subject of several studies [5, 6, 4, 7, 9, 13, 15, 17, 19, 20, 26].

A Boolean function $f \in \mathcal{B}_n$ is called symmetric if it is invariant under the action of the symmetric group S_n of n symbols, that is, if

$$f\left(X_{\sigma(1)}, \ldots, X_{\sigma(n)}\right) = f(X_1, \ldots, X_n)$$

for every $\sigma \in S_n$. On the other hand, a Boolean function $f \in \mathcal{B}_n$ is called rotation symmetric if it is invariant under the action of the cyclic group $\mathbb{Z}_n$. Explicitely, if C_n is the representation of $\mathbb{Z}_n$ in S_n, then

$$f\left(X_{\sigma(1)}, \ldots, X_{\sigma(n)}\right) = f(X_1, \ldots, X_n)$$

for every $\sigma \in C_n$.

It is well-known that the ANF of a symmetric Boolean function $f \in \mathcal{B}_n$ has the form

$$f = \boldsymbol{e}_{n,k_1} \oplus \boldsymbol{e}_{n,k_2} \oplus \cdots \oplus \boldsymbol{e}_{n,k_s} \tag{1.4}$$

where $0 \leq k_1 < \cdots < k_s$ are integers and $\boldsymbol{e}_{n,k}$ represents the n-variable elementary symmetric polynomial of degree k. For simplicity, the notation $\boldsymbol{e}_{n,[k_1,\ldots,k_s]}$ is used to represent the right-hand side of (1.4). It is known that if $0 \leq k_1 < \cdots < k_s$ are fixed integers, then the sequence $\{S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})\}_n$ satisfies a linear recurrence with constant coefficients [1, 5], in other words, it is a C-finite sequence. To be more specific, the sequence $\{S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})\}_n$ satisfies the recurrence whose characteristic polynomial is given by

$$(X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1), \tag{1.5}$$

where $r = \lfloor \log_2(k_s) \rfloor + 1$ and $\Phi_n(X)$ represents the n-th cyclotomic polynomial. The fact that $\{S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})\}_n$ is a C-finite sequence is important, as it implies that the value of the exponential sum can be calculated efficiently provided some initial conditions. This result was extended to Walsh-Hadamard transformations of symmetric Boolean functions in [7] and to every finite field in [8]. Even though the exponential sums (as well as other transformations) of symmetric Boolean functions can be computed efficiently, symmetric Boolean functions are often avoided in cryptographic applications because of security concerns.

Rotation symmetric Boolean functions were introduced by Pieprzyk and Qu in the late 1990's [26]. They showed that these functions are useful, among other things, in the design of fast hashing algorithms with strong cryptographic properties. Their work prompted further research on this class of functions. In 2006, 9-variable Boolean functions with nonlinearity 241 where found in the class of rotation symmetric Boolean functions [19]. To find such Boolean functions was an open problem for more than three decades before their discovery. In [9], T. Cusick proved that, as in the case of symmetric Boolean functions, sequences of weights of rotation symmetric Boolean functions are C-finite. Cusick's result was later generalized to Walsh-Hadamard transformations [7] and to every finite field [3]. His result implies that, as in the case of symmetric Boolean functions, values of exponential sums of rotation symmetric Boolean functions can be computed efficiently (provided some initial conditions). However, we still do not have an explicit formula like (1.5) for the case of rotation symmetric Boolean functions and we do not know a priori the order of the recurrence.

The ANF of a rotation symmetric Boolean function is, as in the case of symmetric Boolean functions, well-understood. Let $1 < j_1 < \cdots < j_s$ be integers. Rotation symmetric Boolean functions of the form

$$R_{j_1,\ldots,j_s}(n) = X_1 X_{j_1} \cdots X_{j_s} \oplus X_2 X_{j_1+1} \cdots X_{j_s+1} \oplus \cdots \oplus X_n X_{j_1-1} \cdots X_{j_s-1}, \tag{1.6}$$

where none of the terms overlap or

$$R_{j_1,\ldots,j_s}(n) = X_1 X_{j_1} \cdots X_{j_s} \oplus \cdots \oplus X_k X_{j_1+k} \cdots X_{j_s+k} \tag{1.7}$$

where $X_{k+1}X_{j_1+k+1}\cdots X_{j_s+k+1}$ is the first term overlapping one of the previous terms; are called a *monomial rotation symmetric Boolean functions* (the indices are taken modulo n with the complete system of residues $\{1, 2, \ldots, n\}$). The *period* of a monomial rotation Boolean function is the amount of terms it has. The ANF of a rotation symmetric Boolean function is a combination of monomial rotation symmetric Boolean functions. We say that $R_{j_1,\ldots,j_s}(n)$ is *long cycle* if its period is n and *short cycle* if its period is less than n. For instance, the rotation

$$R_{2,3}(4) = X_1X_2X_3 \oplus X_2X_3X_4 \oplus X_3X_4X_1 \oplus X_4X_1X_2$$

is an example of a long cycle, while

$$R_3(4) = X_1X_3 \oplus X_2X_4$$

is an example of a short cycle. The ANF of a rotation symmetric Boolean function is a combination of rotation monomial symmetric Boolean functions

As previously discussed, families of Boolean functions that are invariant under the action of a certain (fixed) finite group are used, among other things, to make searches of Boolean functions with good cryptographic attributes, thus it is natural to ask how many of such functions are there. In [27], Stănică and Maitra provided the number of rotation symmetric Boolean functions in $\mathfrak{B}_n$. They found this number to be given by 2^{g_n} where

$$g_n = \frac{1}{n}\sum_{d|n}\phi(d)2^{n/d}, \tag{1.8}$$

and ϕ is the Euler's totient function (see [27, Th. 3]). Stănică and Maitra went further and provided the count of short cycles and the count of long cycles (see [27, Th. 9]). They also presented a study of rotation symmetric functions with cryptographic significance. In particular, they studied rotation symmetric bent functions and found all homogeneous rotation symmetric Boolean functions in 10 variables of degree 2 that are bent functions. Furthermore, they conjectured the following:

There are no homogeneous rotation symmetric Boolean bent functions of degree bigger than 2.

This conjecture remains an open problem. See [27, Conj. 12] for more details.

In this article we are interested in another family of Boolean functions that are invariant under the action of the subgroup of n/k elements of C_n (observe that k must divide n). These functions are called k-rotation Boolean functions. They are a generalization of the concept of rotation Boolean functions and were introduced by Kavut and Yücel in [21]. Kavut and Yücel found 9-variable Boolean functions with nonlinearity 242 in the class of 3-rotation symmetric Boolean functions, which is an improvement over the bound presented in [19].

In this article, we characterize when a monomial k-rotation symmetric Boolean function is a short k-cycle (to be defined in the next section). We do this by exhibiting an explicit generator for them. These results can be proved using elementary machinery and are generalizations of the ones presented in [27] for regular rotation monomial Boolean functions. The results also generalize the count presented in [10, 14] for monomial k-rotation symmetric Boolean functions of degree 3 for $k = 2, 3$. Characterizing short k-cycles is important, as they often need to be excluded in results related to affine equivalency and the recursivity of Hamming weights of k-rotations symmetric Boolean functions [11, 12]

We finish this introduction by saying that the idea of a Boolean function can be easily extended to any Galois field $\mathbb{F}_q$ with q a power of a prime p. A function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is called a q-ary function in n variables. The set of all q-ary functions in n variables is denoted by $\mathfrak{B}_{n,q}$. Observe that $\mathfrak{B}_{n,2} = \mathfrak{B}_n$. The concepts of symmetric, rotation symmetric, k-rotation symmetric, and more general, G-invariant q-ary function, can also be extended to $\mathbb{F}_q$ by making the appropiate adjustments. Today, many cryptographic properties have been extended to characteristic beyond two [3, 8, 16, 23, 24, 25]. In the last section of this article, we generalize our main results from $\mathbb{F}_2$ to every finite field.

2. Preliminaries

Let k and n be a positive integers with $k \leq n$. Consider the set of variables $\{X_1, \ldots, X_n\}$. The k-shift operator $E_{n,k}$ is defined as

$$E_{n,k}(X_j) = \begin{cases} X_{j+k}, & \text{if } j+k \leq n \\ X_{j+k-n}, & \text{if } j+k > n. \end{cases} \tag{2.1}$$

This map can be extended to tuples $(X_1, \ldots, X_n)$ via

$$E_{n,k}(X_1, \ldots, X_n) = (E_{n,k}(X_1), \ldots, E_{n,k}(X_n)). \tag{2.2}$$

A Boolean function $f \in \mathcal{B}_n$ is called a k-rotation symmetric Boolean function if

$$f(E_{n,k}^{\ell}(X_1, \ldots, X_n)) = f(X_1, \ldots, X_n)$$

for every $0 \leq \ell \leq n$.

Observe that k-rotation symmetric Boolean functions are fixed under the action of the subgroup $\langle k \rangle$ of $\mathbb{Z}_n$. This subgroup can be identified with the subgroup of C_n generated by σ_n^k where σ_n is the rotation

$$\sigma_n = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$$

(C_n is the copy of $\mathbb{Z}_n$ in S_n). Thus if $\gcd(k, n) = 1$, then every k-rotation symmetric Boolean function is in fact a regular rotation symmetric Boolean function. Furthermore, if $\gcd(k, n) = d > 1$, then every k-rotation symmetric Boolean function is a d-rotation symmetric Boolean function. Because of this, we only consider k-rotation symmetric Boolean functions when k divides n.

Let $\ell, m, n \in \mathbb{N}$ with $\ell \leq n$ and $m \leq n/k$. Consider the expression

$$\bigoplus_{j=0}^{m-1} X_{t_1+jk} X_{t_2+jk} \cdots X_{t_\ell+jk}. \tag{2.3}$$

If (2.3) is fixed by the rotation σ_n^k, then we call this expression a *monomial k-rotation symmetric Boolean function* (or monomial k-rotation for short). Any of the terms of (2.3) is called a *generator* for the monomial$k$-rotation. If m is the smallest positive integer that satisfies such condition, then m is called the *period* or *length* of the monomial k-rotation. The polynomial (2.3) is called

(1) a *short cycle monomial k-rotation* of size m if $m < n/k$,
(2) a *long cycle monomial k-rotation* if $m = n/k$.

For simplicity of the writing, we often use the term short (long) k-cycle to express that the Boolean function considered is a short (long) cycle monomial k-rotation. We also use the notation $k\text{-}R_{t_1,t_2,\cdots,t_\ell}(n)$ to represent (2.3).

As discussed in the introduction, families of Boolean functions that are invariant under the action of a certain (fixed) finite group are used, among other things, to make searches of Boolean functions with good cryptographic attributes, thus it is natural to ask how many of such functions are there. An answer to this question uses Burnside's lemma.

Theorem 2.1 (Burnside's lemma)**.** *Let G be a group of permutations acting on a set S. The number of orbits induced on S is given by*

$$\frac{1}{|G|} \sum_{\sigma \in G} |\operatorname{Fix}_S(\sigma)|, \tag{2.4}$$

where $\operatorname{Fix}_S(\sigma) = \{x \in S : \sigma(x) = x\}$.

Suppose that $G < S_n$ acts on $\mathbb{F}_2^n$. This action induces a partition of $\mathbb{F}_2^n$ into orbits. For example, the partition of $\mathbb{F}_2^6$ induced by the action of C_6 is given in Table 1. The G-invariant Boolean functions are characterized by being the Boolean functions that have a constant value on each orbit of the partition induced by the action of G on $\mathbb{F}_2^n$. It is clear that if the partition of $\mathbb{F}_2^n$ generated by the action of G has N orbits, then the number of G-invariant Boolean functions in n variables is given by 2^N. For example, there are 2^{14} rotation symmetric Boolean functions in 6 variables (this a significantly smaller number than the amount of all Boolean functions in 6 variables). The number N can by computed using Burnside's lemma.

Let g_n be number of orbits in the partition of $\mathbb{F}_2^n$ generated by the action of C_n. By using Burnside's lemma, Stănică and Maitra [27] found the value of g_n to be (1.8). Kavut and Yücel showed that a similar result holds for k-rotation symmetric Boolean function [21]. We present the result in a more general setting. The proof presented follows the standard machinery presented in [27], which is based on the fact that we are working with cyclic groups.

TABLE 1. Orbits of $\mathbb{F}_2^6$ corresponding to the action of C_6.

orbit 1:	(0, 0, 0, 0, 0, 0)		
orbit 2:	(0, 0, 0, 0, 0, 1),	(0, 0, 0, 0, 1, 0),	(0, 0, 0, 1, 0, 0),
	(0, 0, 1,0, 0, 0),	(0, 1, 0, 0, 0, 0),	(1, 0, 0, 0, 0, 0)
orbit 3:	(0, 0, 0, 0, 1, 1),	(0, 0, 0, 1, 1, 0),	(0, 0, 1, 1, 0, 0),
	(0, 1, 1, 0, 0, 0),	(1, 0, 0, 0, 0, 1),	(1, 1, 0, 0, 0, 0)
orbit 4:	(0, 0, 0, 1, 0, 1),	(0, 0, 1, 0, 1, 0),	(0, 1, 0, 0, 0, 1),
	(0, 1, 0, 1, 0, 0),	(1, 0, 0, 0, 1, 0),	(1, 0, 1, 0, 0, 0)
orbit 5:	(0, 0, 1, 0, 0, 1),	(0, 1, 0, 0, 1, 0),	(1, 0, 0, 1, 0, 0)
orbit 6:	(0, 0, 0, 1, 1, 1),	(0, 0, 1, 1, 1, 0),	(0, 1, 1, 1, 0, 0),
	(1, 0, 0, 0, 1, 1),	(1, 1, 0, 0, 0, 1),	(1, 1, 1, 0, 0, 0)
orbit 7:	(0, 0, 1, 1, 0, 1),	(0, 1, 0, 0, 1, 1),	(0, 1, 1, 0, 1, 0),
	(1, 0, 0, 1, 1, 0),	(1, 0, 1, 0, 0, 1),	(1, 1, 0, 1, 0, 0)
orbit 8:	(0, 0, 1, 0, 1, 1),	(0, 1, 0, 1, 1, 0),	(0, 1, 1, 0, 0, 1),
	(1, 0, 0, 1, 0, 1),	(1, 0, 1, 1, 0, 0),	(1, 1, 0, 0, 1, 0)
orbit 9:	(0, 1, 0, 1, 0, 1),	(1, 0, 1, 0, 1, 0)	
orbit 10:	(0, 0, 1, 1, 1, 1),	(0, 1, 1, 1, 1, 0),	(1, 0, 0, 1, 1, 1),
	(1, 1, 0, 0, 1, 1),	(1, 1, 1, 0, 0, 1),	(1, 1, 1, 1, 0, 0)
orbit 11:	(0, 1, 0, 1, 1, 1),	(0, 1, 1, 1, 0, 1),	(1, 0, 1, 0, 1, 1),
	(1, 0, 1, 1, 1, 0),	(1, 1, 0, 1, 0, 1),	(1, 1, 1, 0, 1, 0)
orbit 12:	(0, 1, 1, 0, 1, 1),	(1, 0, 1, 1, 0, 1),	(1, 1, 0, 1, 1, 0)
orbit 13:	(0, 1, 1, 1, 1, 1),	(1, 0, 1, 1, 1, 1),	(1, 1, 0, 1, 1, 1),
	(1, 1, 1, 0, 1, 1),	(1, 1, 1, 1, 0, 1),	(1, 1, 1, 1, 1, 0)
orbit 14:	(1, 1, 1, 1, 1, 1).		

Proposition 2.2. *Suppose that n is a positive integer and k a positive divisor of n. Let $S = \{\alpha_0, \ldots, \alpha_{L-1}\}$ be any set of L symbols where L is a fixed positive integer. Consider the set $\mathbb{T}_n = S^n$ of all n-tuples of elements of S. The number of orbits in the partition of $\mathbb{T}_n$ induced by the action of $\langle \sigma_n^k \rangle$ is given by*

$$\frac{k}{n} \sum_{d \,|\, n/k} \phi(d) L^{n/d}, \tag{2.5}$$

where ϕ is the Euler's totient function.

Proof. The permutation σ_n^{kj} is descomposed into $\gcd(n, kj) = k \gcd(n/k, j)$ disjoint cycles, each with length

$$\frac{n}{\gcd(n, kj)} = \frac{n/k}{\gcd(n/k, j)}.$$

In order for $\boldsymbol{\delta} \in \mathbb{T}_n$ to be fixed by σ_n^{kj} each of the entries corresponding to a disjoint cycle of σ_n^{kj} must be the same. For example, if $n = 6$, $k = 2$ and $j = 2$, then the disjoint cycle decomposition of the permutation σ_6^4 is

$$\sigma_6^4 = (1\ 5\ 3)(2\ 6\ 4).$$

Thus, if $\boldsymbol{\delta} \in \mathbb{F}_2^6$ is to be fixed by σ_6^4, then its first, third and fifth entries must be the equal and its second, fourth and sixth entries must also be equal. In other words, $\boldsymbol{\delta}$ must have the form $(\alpha_i, \alpha_j, \alpha_i, \alpha_j, \alpha_i, \alpha_j)$. Since σ_n^{kj} has $k \gcd(n/k, j)$ disjoint cycles in its cycle decomposition, it follows that σ_n^{kj} has $L^{k \gcd(n/k, j)}$ fixed

points in $\mathbb{T}_n$. Burnside's lemma implies that number of orbits is given by

$$\begin{aligned}\frac{1}{n/k}\sum_{j=1}^{n/k} L^{k\gcd(n/k,j)} &= \frac{k}{n}\sum_{d\,|\,n/k}\ \sum_{j,\gcd(n/k,j)=d}^{n/k} L^{kd}\\ &= \frac{k}{n}\sum_{d\,|\,n/k} L^{kd}\sum_{j,\gcd(n/(kd),j)=1} 1\\ &= \frac{k}{n}\sum_{d\,|\,n/k}\phi\left(\frac{n}{kd}\right)L^{kd}\\ &= \frac{k}{n}\sum_{d\,|\,n/k}\phi\left(d\right)L^{n/d}.\end{aligned}$$

This concludes the proof. □

Corollary 2.3. *Let n be a positive integer and k a positive divisor of n. Suppose that p is a prime integer and r a positive integer. The number of k-rotation symmetric p^r-ary functions in $\mathfrak{B}_{n,p^r}$ is given by $p^{rg_{n,k,p^r}}$, where*

$$g_{n,k,p^r} = \frac{k}{n}\sum_{d\,|\,n/k}\phi(d)p^{rn/d},$$

We point out that there is a one to one correspondence between the orbits in the partition of $\mathbb{F}_2^n$ indunced by the action of $\langle\sigma_n^k\rangle$ and monomial k-rotation. If $\boldsymbol{\delta} = (\delta_1,\ldots,\delta_n)\in\mathbb{F}_2^n$, then define $(X_1\cdots X_n)^{\boldsymbol{\delta}}$ to be

$$(X_1\cdots X_n)^{\boldsymbol{\delta}} = X_1^{\delta_1}\cdots X_n^{\delta_n}.$$

Given $G<S_n$, define $\mathcal{O}_G(\mathbb{F}_2^n)$ to be the set of all distinct orbits induced by the action of G on $\mathbb{F}_2^n$. Define, for $\mathcal{O}\in\mathcal{O}_G(\mathbb{F}_2^n)$, the Boolean polynomial

$$f_{\mathcal{O}}(X_1,\cdots,X_n) = \bigoplus_{\boldsymbol{\delta}\in\mathcal{O}}(X_1\cdots X_n)^{\boldsymbol{\delta}}. \tag{2.6}$$

For example, if $\mathcal{O}$ is the fifth orbit in Table 1, then

$$f_{\mathcal{O}}(\mathbf{X}) = X_1X_4\oplus X_2X_5\oplus X_3X_6,$$

which is a rotation symmetric monomial ($G=C_6$ in this example). It is not hard to see that, when $G=\langle\sigma_n^k\rangle$, the polynomial (2.6) is always a k-rotation symmetric monomial.

The map from $\mathcal{O}_{\langle\sigma_n^k\rangle}(\mathbb{F}_2^n)$ to $\mathfrak{B}_n$ given by $\mathcal{O}\to f_{\mathcal{O}}$ is a one to one correspondence between $\mathcal{O}_{\langle\sigma_n^k\rangle}(\mathbb{F}_2^n)$ and the set of all distinct k-rotation symmetric monomials. This correspondence was exploited by Stănică and Maitra when they provided the count of long cycles and the count of short cycles for regular rotation symmetric Boolean functions [27]. Observe that this one to one correspondence also holds if we replace $\mathbb{F}_2$ with any Galois field $\mathbb{F}_{p^r}$ (p prime).

In the next section we will provide generators for short k-cycles. We then use these generators to count short k-cycles. Our results are presented in terms of k-rotation symmetric monomials instead of tuples in an orbit, but the same results can be obtained by studying tuples instead of polynomials.

3. Generators for short cycles

We already defined long cycle and short cycle k-rotation symmetric Boolean functions. Our first result concerns about the relation between the length of the k-cycle (i.e. its period m) and the number of variables n. This result is a straight forward result from group actions and it is not surprising.

Lemma 3.1. *Let $k,\ell,n\in\mathbb{N}$ with $\ell<n$ and $k|n$. If k-$R_{t_1t_2,\cdots,t_\ell}(n)$ is a short cycle of size m, then $m|n/k$.*

Proof. Recall that k-rotation symmetric Boolean functions are those functions in $\mathfrak{B}_n$ that are fixed under the action of the subgroup $H=\langle\sigma_n^k\rangle$ of the cyclic cyclic group $C_n=\langle\sigma_n\rangle$. The terms of the rotation generated by the monomial $X_{t_1}X_{t_2}\cdots X_{t_\ell}$ are precisely the elements of $\mathcal{O}(X_{t_1}X_{t_2}\cdots X_{t_\ell})$, which represents the orbit of $X_{t_1}X_{t_2}\cdots X_{t_\ell}$ under the action of H. Thus m divides the order of H, which is n/k. This concludes the proof. □

A natural step now is to find a way to detect a short k-cycle by analyzing its generators. We start with the following auxiliary result.

Lemma 3.2. *Let n and k be natural numbers and k-$R_{t_1,t_2,\ldots,t_\ell}(n)$ be a k-rotation with*

$$1 \leq t_1 < t_2 < \cdots < t_\ell \leq n.$$

If there is $t_j \equiv t \mod k$, then at least one of the terms of k-$R_{t_1,t_2,\ldots,t_\ell}$ has the variable X_t in it.

Proof. Suppose that there is a t_j such that $t_j \equiv t \mod k$. Then, there is a non-negative integer a such that $t_j = t + ak$. Also, since k divides n, there is a non-negative integer b such that $n = bk$. Let $v = b - a$. Observe that

$$\sigma_n^{kv} \cdot \left(X_{t_1} \cdots X_{t_j} \cdots X_{t_\ell}\right) = X_{t_1+kv} \cdots X_{t_j+kv} \cdots X_{t_{\ell+kv}}.$$

In particular,

$$X_{t_j+kv} = X_{t+ak+k(b-a)} = X_{t+kb} = X_{t+n} = X_t.$$

This concludes the proof. □

The next result identifies explicit generators for short k-cycles of length m.

Theorem 3.3. *Let ℓ, k and n be natural numbers with $\ell < n$. If k-$R_{t_1,\cdots,t_\ell}(n)$ is a short k-cycle of length m, then $n/(km)$ divides ℓ (the degree of k-$R_{t_1,\ldots,t_\ell}(n)$) and there are integers $1 \leq s_1 < s_2 < \cdots < s_{q_m} \leq mk$, with $q_m = q_m(k,\ell,n) = mk\ell/n$ and $1 \leq s_1 \leq k$, such that*

$$\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk} X_{s_2+jmk} \cdots X_{s_{q_m}+jmk} \tag{3.1}$$

is a generator of k-$R_{t_1,\ldots,t_\ell}(n)$.

Proof. Suppose that k-$R_{t_1,\ldots,t_\ell}(n)$ is a short k-cyle of length m. Then m divides n/k. Let $d = n/(mk)$. By Lemma 3.2 there is a term that has X_{s_1} in it, where $s_1 = \min\{s : t_j \equiv s \mod k\}$ (understanding that the complete reduced residue system mod k is $\{1, 2, \cdots, k\}$). Suppose that $X_{s_1}X_{s_2}\cdots X_{s_\ell}$ is such term. This term is also a generator of the k-rotation k-$R_{t_1,\ldots,t_\ell}(n)$ with $1 \leq s_1 \cdots < s_\ell \leq n$ and $1 \leq s_1 \leq k$. Thus the terms of k-$R_{t_1,\ldots,t_\ell}(n)$ are given by

$$\begin{array}{rcl} X_{s_1}X_{s_2} & \cdots & X_{s_{\ell-1}}X_{s_\ell} \\ X_{s_1+k}X_{s_2+k} & \cdots & X_{s_{\ell-1}+k}X_{s_\ell+k} \\ X_{s_1+2k}X_{s_2+2k} & \cdots & X_{s_{\ell-1}+2k}X_{s_\ell+2k} \\ & \vdots & \\ X_{s_1+(m-1)k}X_{s_2+(m-1)k} & \cdots & X_{s_{\ell-1}+(m-1)k}X_{s_\ell+(m-1)k}, \end{array} \tag{3.2}$$

where it is understood that the indices of variables are to be taken mod n with reduced residue system $\{1, 2, \ldots, n\}$. If we continue adding k to the subscripts the next term is

$$X_{s_1+mk}X_{s_2+mk}\cdots X_{s_{\ell-1}+mk}X_{s_\ell+mk}. \tag{3.3}$$

However, k-$R_{t_1,\ldots,t_\ell}(n)$ is a short k-cycle of length m (hypothesis), thus term (3.3) is equal to one of the terms on the list (3.2). In other words, there is $i \in \{2, 3, \ldots, \ell\}$ such that

$$\begin{array}{rcl} s_i & = & s_1 + mk \\ s_{i+j} & = & s_{1+j} + mk \text{ for } j \in \{1, 2, \ldots, \ell - i\} \\ n + s_j & = & s_{\ell-i+1+j} + mk \text{ for } j \in \{1, 2, \ldots, i-1\}. \end{array} \tag{3.4}$$

Therefore, the term (3.3) is given by

$$X_{s_i}X_{s_{i+1}}\cdots X_{s_\ell}\underbrace{X_{s_1}X_{s_2}\cdots X_{s_{i-1}}}_{i-1 \text{ variables}}$$

and it is also a generator for k-$R_{t_1,\ldots,t_\ell}(n)$.

The terms of k-$R_{t_1,\ldots,t_\ell}(n)$ can now be re-written as

$$\begin{array}{rcl} X_{s_i}X_{s_{i+1}} & \cdots & X_{s_\ell}X_{s_1}X_{s_2}\cdots X_{s_{i-1}} \\ X_{s_i+k}X_{s_{i+1}+k} & \cdots & X_{s_\ell+1}X_{s_1+k}X_{s_2+k}\cdots X_{s_{i-1}+k} \\ & \vdots & \\ X_{s_i+(m-1)k}X_{s_{i+1}+(m-1)k} & \cdots & X_{s_\ell+(m-1)k}X_{s_1+(m-1)k}X_{s_2+(m-1)k}\cdots X_{s_{i-1}+(m-1)k}. \end{array}$$

After applying σ_n^{mk} to $X_{s_i}X_{s_{i+1}}\cdots X_{s_\ell}X_{s_1}X_{s_2}\cdots X_{s_{i-1}}$ we get

$$X_{s_i+mk}X_{s_{i+1}+mk}\cdots X_{s_\ell+mk}\underbrace{X_{s_1+mk}X_{s_2+mk}\cdots X_{s_{i-1}+mk}}_{i-1 \text{ variables}}$$

and arguing as before (see (3.4)) we see that this term has the form

$$X_{s_{2i-1}}\cdots X_{s_\ell}\underbrace{X_{s_1}X_{s_2}\cdots X_{s_{i-1}}}_{i-1 \text{ variables}}\underbrace{X_{s_1+mk}X_{s_2+mk}\cdots_{s_{i-1}+mk}}_{i-1 \text{ variables}}. \tag{3.5}$$

The term (3.5) is also a generator for k-$R_{t_1,\ldots,t_\ell}(n)$.

Continue with this process to get

$$X_{s_1}X_{s_2}\cdots X_{s_{i-1}}X_{s_1+mk}X_{s_2+mk}\cdots X_{s_{i-1}+mk}\cdots X_{s_1+(d-1)mk}X_{s_2+(d-1)mk}\cdots X_{s_{i-1}+(d-1)mk}$$

is a generator of k-$R_{t_1,t_2,\ldots,t_\ell}(n)$. Observe that

$$\ell = d(i-1) = \frac{n}{mk}(i-1).$$

Let $q := i-1 = \frac{mk\ell}{n}$. Since $s_{q+1} = s_i = s_1 + mk$, then $1 \leq s_1 < \cdots < s_q \leq mk$ and

$$\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk}X_{s_2+jmk}\cdots X_{s_q+jmk}$$

is a generator of k-$R_{t_1,\ldots,t_\ell}(n)$. □

Example 3.4. Consider the 4-rotation given by 4-$R_{6,7,22,23}(32)$. This is a short 4-cycle of length 4. Explicitly,

$$\begin{array}{rcl} 4\text{-}R_{6,7,22,23}(32) & = & X_6X_7X_{22}X_{23} \oplus X_{10}X_{11}X_{26}X_{27} \oplus \\ & & X_{14}X_{15}X_{30}X_{31} \oplus X_{18}X_{19}X_2X_3 \end{array}$$

In this case, $q_4(4,4,32)$ is given by

$$q_4 = \frac{4\times 4\times 4}{32} = 2.$$

According to the previous theorem, there are integers s_1, s_2 satisfying $1 \leq s_1 \leq 4$ and $1 \leq s_1 < s_2 \leq 16$ such that

$$\prod_{j=0}^{1} X_{s_1+16j}X_{s_2+16j} = X_{s_1}X_{s_2}X_{s_1+16}X_{s_2+16}$$

is a generator of 4-$R_{6,7,22,23}(32)$. Indeed, this generator is given by $X_2X_3X_{18}X_{19}$.

Observe that Theorem 3.3 states that if a monomial k-rotation is of length m, then it must have a generator of the form (3.1). In other words, the short k-cycle must have the form

$$\bigoplus_{i=0}^{m-1}\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+(jm+i)k}X_{s_2+(jm+i)k}\cdots X_{s_{q_m}+(jm+i)k}$$

The converse is not true, that is, having a generator (3.1) does not implies that we have a short k-cycle with period m. What is true is that if a monomial k-rotation has a generator of type (3.1), then the length of the

cycle is a divisor of m. To see this, observe that, by performing the operation of mod n on the indices, we have

$$\begin{aligned}
\sigma_n^{mk} \cdot \prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk}X_{s_2+jmk}\cdots X_{s_{q_m}+jmk} &= \prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+(j+1)mk}X_{s_2+(j+1)mk}\cdots X_{s_{q_m}+(j+1)mk} \\
&= \prod_{j=1}^{\frac{n}{mk}} X_{s_1+jmk}X_{s_2+jmk}\cdots X_{s_{q_m}+jmk} \\
&= \prod_{j=1}^{\frac{n}{mk}-1} X_{s_1+jmk}X_{s_2+jmk}\cdots X_{s_{q_m}+jmk} \\
&\quad \times X_{s_1+(n/(mk))mk}X_{s_2+(n/(mk))mk}\cdots X_{s_{q_m}+(n/(mk))mk} \\
&= \prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk}X_{s_2+jmk}\cdots X_{s_{q_m}+jmk},
\end{aligned}$$

which implies

$$\sigma_n^{mk} \in \mathrm{Stab}\left(\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk}X_{s_2+jmk}\cdots X_{s_{q_m}+jmk}\right). \tag{3.6}$$

But any stabilizer is a subgroup of $H = \langle \sigma_n^k \rangle$. Since (3.6) is true, then it follows that the length of the cycle is a divisor of m.

In the next section we will used Theorem 3.3 to provide a count of the number of short k-cycles of length m.

4. Count of short k-cycles

Let m be a divisor of n/k such that $n/(mk)$ divides ℓ. In this section we will prove a formula for the number of short k-cycles $k\text{-}R_{t_1,\ldots,t_\ell}(n)$ with period m. We start the following definition.

Definition 4.1. Suppose that ℓ, k and n are positive integers with $\ell < n$. Let m be a divisor of n/k such that $n/(km)$ divides ℓ. Then,

$$\begin{aligned}
q_m(n,\ell,k) &= \frac{mk\ell}{n}, \\
D_m(n,\ell,k) &= \{1 \le d < m \,:\, d|m \text{ and } q_d \in \mathbb{N}\} \text{ for } m \ge 2, \\
\mathrm{C}_m(n,\ell,k) &= \{k\text{-}R_{r_1,\ldots,r_\ell}(n) \,:\, k\text{-}R_{r_1,\ldots,r_\ell}(n) \text{ is a } k\text{-cycle of length } m\}.
\end{aligned} \tag{4.1}$$

When the context is clear, we write D_m and q_m instead of $D_m(n,\ell,k)$ and $q_m(n,\ell,k)$.

Our goal is to calculate $\#\mathrm{C}_m(n,\ell,k)$. Next is an auxiliary result.

Lemma 4.2. *Let ℓ, k and n be natural numbers with $\ell < n$. Consider a k-cycle of length m with generator given by (3.1). For $1 \le z \le k$, define*

$$[z] = \{s_r \,:\, s_r \equiv z \mod k \quad \text{for } 1 \le r \le q_m\}.$$

Then, the k-cycle has $\#[z]$ terms which contain the variable X_z.

Proof. By previous discussion we know that the k-cycle of length m can be written as

$$\bigoplus_{i=1}^{m} \prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk+ik}X_{s_2+jmk+ik}\cdots X_{s_{q_m}+jmk+ik} \tag{4.2}$$

where $1 \le s_1 < s_2 < \cdots < s_{q_m} \le km$. Let $s_r \in [z]$, then $s_r = z + ak$ for some integer $0 \le a < m$. Take $i = m - a$ in (4.2) and consider the term

$$\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk+(m-a)k}\cdots X_{s_r+jmk+(m-a)k}\cdots X_{s_{q_m}+jmk+(m-a)k}. \tag{4.3}$$

Focus on the variable $X_{s_r+jmk+(m-a)k}$ and let $j = n/(mk) - 1$. Note that

$$\begin{aligned} X_{s_r+jmk+(m-a)k} &= X_{z+ak+\left(\frac{n}{mk}-1\right)mk+(m-a)k} \\ &= X_{z+n} \\ &= X_z. \end{aligned}$$

Thus, X_z is one of the variables of the term (4.3). Furthermore, since $s_r \in [z]$ was arbitrarily chosen, then each element in $[z]$ generates a term of the k-cycle that contains the variable X_z. In other words, the number of times X_z appears as a variable of one of the terms of the k-cycle is bigger than or equal to $\#[z]$.

The converse is also true. If there is a term of (4.2) which has X_z as one of its variables, then there is an $s \in \{s_1, s_2, \cdots, s_{q_m}\}$, a $j \in \{0, 1, 2, \cdots, n/(mk) - 1\}$ and an $i \in \{1, 2, \cdots, m\}$ such that

$$X_{s+jmk+ik} = X_z.$$

It is clear that $s \equiv z \mod k$. This completes the proof. □

Theorem 4.3. *Let ℓ, k and n be natural numbers with $\ell < n$ and k divisor of n. Suppose that m is a divisor of n/k and that $n/(mk)$ divides ℓ. If $D_m = \emptyset$, then the number of short k-cycles of length m is given by*

$$\#\mathrm{C}_m(n, \ell, k) = \sum_{i=1}^{k} \sum_{j=0}^{q_m-1} \frac{1}{q_m - j} \binom{m-1}{q_m - 1 - j} \binom{mk - im}{j} \tag{4.4}$$

Proof. By Theorem 3.3 any short k-cycle of length m has a generator of the form

$$\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk} X_{s_2+jmk} \cdots X_{s_{q_m}+jmk}, \tag{4.5}$$

where $1 \leq s_1 < s_2 < \cdots < s_{q_m} \leq mk$ and $q_m = mk\ell/n \in \mathbb{N}$. By hypothesis $D_m = \emptyset$, thus (4.5) only generates k-cycles of length m. For each generator (4.5), let $S_m := \{s_1, s_2, \ldots, s_{q_m}\}$ and $T_z := \{s \in S_m : s \equiv z \mod k\}$ for $t \geq 1$. We need to count the number of ways of choosing the subscripts $s_1, \ldots, s_{q_m}$ in such a way that (4.5) generates different k-cycles. We proceed by cases.

Case 1: Suppose first that $m < q_m$. Consider first the case when $s_1 = 1$. The cardinality of T_1 must have the form $\#T_1 = m - j$ for some $0 \leq j \leq m - 1$. Observe that

$$\#\{1 \leq s \leq mk : s \not\equiv 1 \mod k\} = mk - m,$$

which implies that there are

$$\binom{mk - m}{q_m - m + j}$$

possible ways of choosing subscripts that are not in T_1. Since $s_1 = 1$, there are

$$\binom{m-1}{m-1-j}$$

ways to choose the rest of the subscripts that are congruent to $1 \mod k$. Thus, there are

$$\binom{m-1}{m-1-j}\binom{mk-m}{q_m-m+j}$$

possible ways to construct the set S_m. Not all of these possibilities generate different k-rotations. Lemma 4.2 implies there are $m-j$ terms in the k-cycle containing the variable X_1. Thus, given $s_1 = 1$ and $\#T_1 = m-j$, the number of ways to construct the set S_m in such a way that (4.5) generates different k-cycles is

$$\frac{1}{m-j}\binom{m-1}{m-1-j}\binom{mk-m}{q_m-m+j}.$$

We conclude that the number of short k-cycles of length m with $s_1 = 1$ is given by

$$\sum_{j=0}^{m-1} \frac{1}{m-j}\binom{m-1}{m-1-j}\binom{mk-m}{q_m-m+j}.$$

Suppose now that $s_1 \neq 1$. Say that $s_1 = i$ where $i \geq 2$ and there are not subscripts in S_m which are congruent to $1, 2, \ldots, i-1 \mod k$. As before, $\#T_i = m - j$ with $0 \leq j \leq m-1$. Also,

$$\#\{1 \leq s \leq mk : s \not\equiv 1, 2, \ldots, i \mod k\} = mk - im,$$

which implies that there are

$$\binom{mk - mi}{q_m - m + j}$$

possible ways of choosing subscripts that are not in T_i (observe that if $i > k - \lfloor q_m/m \rfloor$, then this number is zero). Arguing as before implies that the number of short k-cycles of length m with $s_1 = i$, for $2 \leq i \leq k$ is given by

$$\sum_{j=0}^{m-1} \frac{1}{m-j} \binom{m-1}{m-1-j} \binom{mk - im}{q_m - m + j}.$$

We conclude that number of different k-rotations of length m is

$$\sum_{i=1}^{k} \sum_{j=0}^{m-1} \frac{1}{m-j} \binom{m-1}{m-1-j} \binom{mk - im}{q_m - m + j}. \tag{4.6}$$

A change of variables transforms (4.6) into

$$\sum_{i=1}^{k} \sum_{j=0}^{q_m-1} \frac{1}{q_m-j} \binom{m-1}{q_m-j-1} \binom{mk - im}{j}. \tag{4.7}$$

Case 2: Suppose now that $m > q_m$. The proof of this case follows almost verbatim as the one of the previous case. One difference is that now $\#T_i = q_m - j$ for some $0 \leq j \leq q_m - 1$. A similar argument as before implies that number of different k-rotations of length m is given by (4.7).

This concludes the proof. □

We are now ready for the main result of this section.

Theorem 4.4. *Let ℓ, k and n be natural numbers with $\ell < n$. Suppose that m is a divisor of n/k such that $n/(mk)$ divides ℓ. The number of short k-cycles of length m is given for*

$$\#\mathrm{C}_m(n,\ell,k) = \sum_{i=1}^{k} \sum_{j=0}^{q_m-1} \frac{1}{q_m-j} \binom{m-1}{q_m-1-j} \binom{mk - im}{j} - \sum_{d \in D_m} \frac{d}{m} \#\mathrm{C}_d(n,\ell,k). \tag{4.8}$$

Proof. We know that a short cycle of length m in n variables must have a generator of the form

$$\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk} X_{s_2+jmk} \cdots X_{s_{q_m}+jmk}. \tag{4.9}$$

Moreover, the important part of this generator is the product of its first q_m variables

$$X_{s_1} X_{s_2} X_{s_3} X_{s_4} \cdots X_{s_{q_m-2}} X_{s_{q_m-1}} X_{s_{q_m}}, \tag{4.10}$$

as everything can be expressed in terms of it. If $D_m = \emptyset$, then Theorem 4.3 tell us that the number of short k-cycles of length m is given

$$\sum_{i=1}^{k} \sum_{j=0}^{q_m-1} \frac{1}{q_m-j} \binom{m-1}{q_m-1-j} \binom{mk - im}{j}. \tag{4.11}$$

If $D_m \neq \emptyset$, then (4.9) generates short k-cycles of length m and of length d where $d \in D_m$. Therefore, to count the exact number of short k-cycles of length m, we must subtract to (4.11) a correction related to the short k-cycles of length d for each $d \in D_m$.

Suppose first that $D_m = \{d\}$. Then $d \mid m$, which implies that $q_d \mid q_m$. Group the variables in (4.10) into q_m/q_d groups as follows (the vertical lines are used to appreciate the split of the generator into different groups of variables)

$$X_{s_1} X_{s_2} \cdots X_{s_{q_d}} \,|\, X_{s_{q_d}+1} X_{s_{q_d}+2} \cdots X_{s_{2q_d}} \,|\, \cdots \,|\, X_{s_{q_m-q_d}} X_{s_{q_m-q_d+1}} \cdots X_{s_{q_m}}. \tag{4.12}$$

If (4.12) generates a short k-cycle of length d, then each group from the second to the last can be constructed from the first group. Consider the set T_z used in the proof of Theorem 4.3. Recall that for each $i \in \{1, 2, \ldots, k\}$, the cardinality of T_i can be written as $q_m - j$, where $0 \leq j \leq q_m - 1$ represents the number of subscripts that are not congruent to $i \mod k$. In order to have a short cycle of length d, all the j subscripts that are not congruent to i must be equally distributed in the q_m/q_d groups. Therefore, in the first q_d variables, there must be $j \div (q_m/q_d) = jq_d/q_m$ subscripts that are not congruent to $i \mod k$ and the number of combinations constructed from the q_m variables having length d is

$$\binom{d-1}{q_d - 1 - \frac{jq_d}{q_m}} \binom{dk - id}{j\frac{q_d}{q_m}}.$$

This discussion impliest that the number of k-cycles of length m having $q_m - j$ subscripts congruent to $i \mod k$ is given by

$$\frac{1}{q_m - j}\left[\binom{m-1}{q_m - 1 - j}\binom{mk - im}{j} - \delta_{\mathbb{N}}\left(\frac{jq_d}{q_m}\right)\binom{d-1}{q_d - 1 - \frac{jq_d}{q_m}}\binom{dk - id}{\frac{jq_d}{q_m}}\right], \tag{4.13}$$

where $\delta_S(x) = 1$ if $x \notin S$ and 0 otherwise. By letting i and j run in their respective domains, we obtain that the number of k-rotations having length exactly m is

$$\sum_{i=1}^{k}\sum_{j=0}^{q_m-1} \frac{1}{q_m - j}\binom{m-1}{q_m - 1 - j}\binom{mk - im}{j} - \sum_{i=1}^{k}\sum_{j=0}^{q_m-1} \delta_{\mathbb{N}}\left(\frac{jq_d}{q_m}\right)\frac{1}{q_m - j}\binom{d-1}{q_d - 1 - \frac{jq_d}{q_m}}\binom{dk - id}{\frac{jq_d}{q_m}}. \tag{4.14}$$

The change of variables $u = jq_d/q_m \in \mathbb{N}$ implies

$$\frac{1}{q_m - j} = \frac{1}{q_m - \frac{uq_m}{q_d}} = \frac{q_d}{q_m q_d - uq_m} = \frac{q_d}{q_m(q_d - u)}. \tag{4.15}$$

Combining (4.14) and (4.15) we have that the number of k-rotations of length m when $D_m = \{d\}$ is given by

$$\sum_{i=1}^{k}\sum_{j=0}^{q_m-1} \frac{1}{q_m - j}\binom{m-1}{q_m - 1 - j}\binom{mk - im}{j} - \frac{q_d}{q_m}\sum_{i=1}^{k}\sum_{j=0}^{q_d-1} \frac{1}{q_d - u}\binom{d-1}{q_d - 1 - u}\binom{dk - id}{u}. \tag{4.16}$$

Observe that $q_d/q_m = d/m$, therefore (4.16) is equivalent to

$$\sum_{i=1}^{k}\sum_{j=0}^{q_m-1} \frac{1}{q_m - j}\binom{m-1}{q_m - 1 - j}\binom{mk - im}{j} - \frac{d}{m}\#\mathrm{C}_d(n, k, \ell). \tag{4.17}$$

The case $\#D_m > 1$ follows in a similar manner. That is, to get the number of k-rotations having length m we must subtract

$$\frac{d}{m}\#\mathrm{C}_d(n, \ell, k). \tag{4.18}$$

to (4.11) for any $d \in D_m$. Therefore,

$$\#\mathrm{C}_m(n, \ell, k) = \sum_{i=1}^{k}\sum_{j=0}^{q_m-1} \frac{1}{q_m - j}\binom{m-1}{q_m - 1 - j}\binom{mk - im}{j} - \sum_{d \in D_m}\frac{d}{m}\#\mathrm{C}_d(n, \ell, k). \tag{4.19}$$

This concludes the proof. □

Corollary 4.5. *Let ℓ and n be natural numbers with $\ell < n$. Suppose that m is a divisor of n with the property that n/m divides ℓ. The number of short cycles of length m in n variables and of degree ℓ is given*

by

$$\begin{aligned}\#\mathrm{C}_m(n,\ell,1) &= \frac{1}{q_m}\binom{m-1}{q_m-1} - \sum_{d\in D_m}\frac{d}{m}\#\mathrm{C}_d(n,\ell,1)\\ &= \frac{1}{q_m}\left[\binom{m-1}{q_m-1} - \sum_{d\in D_m} q_d\#\mathrm{C}_d(n,\ell,1)\right].\end{aligned} \tag{4.20}$$

5. Extension of the results to Galois fields $\mathbb{F}_{p^r}$

As mentioned in the introduction, many cryptographic properties have been extended to characteristic beyond two. Thus, it is natural to ask if the results presented so far can be extended to every finite field. The answer is yes!

Let $S=\{\alpha_0,\alpha_1,\alpha_2,\cdots,\alpha_{L-1}\}$ be a set of L symbols where L is a positive integer getter than or equal to 2. Consider the action of $\langle\sigma_n^k\rangle$ on S^n (the set of n-tuples with entries from S). If $\boldsymbol{\alpha}=(\alpha_{j_1},\cdots,\alpha_{j_n})\in S^n$, then we define $(X_1\cdots X_n)^{\boldsymbol{\alpha}}$ to be

$$(X_1\cdots X_n)^{\boldsymbol{\alpha}} = X_1^{\alpha_{j_1}}\cdots X_n^{\alpha_{j_n}}.$$

For example, if $S=\mathbb{F}_4=\mathbb{F}_2(\gamma)=\{0,1,\gamma,\gamma+1\}$ with $\gamma^2=\gamma+1$, then $=\{\alpha_0,\alpha_1,\alpha_2,\alpha_3\}=\{0,1,\gamma,\gamma+1\}$. If we choose $(1,0,\gamma,\gamma)\in S^4=\mathbb{F}_4^4$, then

$$(X_1X_2X_3X_4)^{(1,0,\gamma,\gamma)} = X_1X_3^2X_4^2.$$

If $\mathcal{O}\in\mathcal{O}_{\langle\sigma_n^k\rangle}$, then the polynomial

$$f_{\mathcal{O}}(X_1,\ldots,X_n)=\sum_{\boldsymbol{\alpha}\in\mathcal{O}}(X_1\cdots X_n)^{\boldsymbol{\alpha}}$$

is called a monomial k-rotation over S. For example, let us go back to $S^4=\mathbb{F}_2(\gamma)^4$. The orbits of $(1,\gamma{+}1,0,0)$ and $(\gamma,1+\gamma,\gamma,1+\gamma)$ under the action of $\langle\sigma_n\rangle$ are given by

$$\begin{aligned}\mathcal{O}_1 &= \mathcal{O}((1,\gamma+1,0,0)) = \{(1,\gamma+1,0,0),(0,1,\gamma+1,0),(0,0,1,\gamma+1),(\gamma+1,0,0,1)\}.\\ \mathcal{O}_2 &= \mathcal{O}((\gamma,1+\gamma,\gamma,1+\gamma)) = \{(\gamma,1+\gamma,\gamma,1+\gamma),(1+\gamma,\gamma,1+\gamma,\gamma)\}.\end{aligned}$$

Thus,

$$\begin{aligned}f_{\mathcal{O}_1}(\mathbf{X}) &= X_1X_2^3+X_2X_3^3+X_3X_4^3+X_4X_1^3\\ f_{\mathcal{O}_2}(\mathbf{X}) &= X_1^2X_2^3X_3^2X_4^3+X_1^3X_2^2X_3^3X_4^2\end{aligned} \tag{5.1}$$

are examples of 1-rotation monomials over $\mathbb{F}_4$ (observe that $k=1$ in this case). We say that a monomial k-rotation $f_{\mathcal{O}}$ over S is a long k-cycle if the corresponding orbit $\mathcal{O}$ has length n/k. Otherwise, we say that $f_{\mathcal{O}}$ is a short cycle. For instance, $f_{\mathcal{O}_1}$ is an example of a long k-cycle while $f_{\mathcal{O}_2}$ is a short k-cycle.

As before, any term of a monomial k-rotation is called a *generator* of it. For example, any of the terms on list

$$X_1X_2^3,\ \ X_2X_3^3,\ \ X_3X_4^3,\ \ X_4X_1^3,$$

is a generator of $f_{\mathcal{O}_1}$. We use the notation $k\text{-}R_{s_1^{e_1},\ldots,s_\ell^{e_\ell}}(n)$ to represent the monomial k-rotation in n variables over S generated by $X_{s_1}^{e_1}\cdots X_{s_\ell}^{e_\ell}$. For example, $1\text{-}R_{1^2,2^3,3^2,4^3}(4)$ represents the polynomial $f_{\mathcal{O}_2}$ in (5.1). Finally, Definition 4.1 in this setting is the following.

Definition 5.1. Suppose that ℓ, k and n are positive integers with $\ell<n$. Let $S=\{\alpha_0,\ldots,\alpha_{L-1}\}$ be a set of L elements. Suppose that $\langle\sigma_n^k\rangle$ acts on S^n. Let m be a divisor of n/k such that $n/(km)$ divides ℓ. Then,

$$\begin{aligned}q_m^L(n,\ell,k) &= \frac{mk\ell}{n},\\ D_m^L(n,\ell,k) &= \{1\le d<m\,:\,d|m \text{ and } q_d^L\in\mathbb{N}\} \text{ for } m\ge 2,\\ \mathrm{C}_m^L(n,\ell,k) &= \{k\text{-}R_{r_1^{e_1},\ldots,r_\ell^{e_\ell}}(n)\,:\,k\text{-}R_{r_1^{e_1},\ldots,r_\ell^{e_\ell}}(n) \text{ is a } k\text{-cycle of length } m\}.\end{aligned} \tag{5.2}$$

With all this at hand, we can now provide the extensions of the main results beyond $\mathbb{F}_2$. Theorem 3.3 can be written in general terms as follows.

Theorem 5.2. *Let ℓ, k and n be natural numbers with $\ell < n$. Suppose that $\langle \sigma_n^k \rangle$ acts on $S = \{\alpha_0, \ldots, \alpha_L\}$. If k-$R_{t_1^{r_1},\cdots,t_\ell^{r_\ell}}(n)$ is a short k-cycle of length m, then $n/(km)$ divides ℓ. Furthermore, if*

$$q_m = q_m(k, \ell, n) = mk\ell/n,$$

then there are integers $1 \leq s_1 < s_2 < \cdots < s_{q_m} \leq mk$ and $n_1, \ldots, n_{q_m} \in \{1, 2, \ldots, L-1\}$, with $1 \leq s_1 \leq k$, such that

$$\prod_{j=0}^{\frac{n}{mk}-1} X_{s_1+jmk}^{n_1} X_{s_2+jmk}^{n_2} \cdots X_{s_{q_m}+jmk}^{n_{q_m}} \tag{5.3}$$

is a generator of k-$R_{t_1^{r_1},\ldots,t_\ell^{r_\ell}}(n)$.

Theorem 4.4 can be extended as follows.

Theorem 5.3. *Let ℓ, k and n be natural numbers with $\ell < n$. Suppose that $\langle \sigma_n^k \rangle$ acts on $S = \{\alpha_0, \ldots, \alpha_L\}$. The number of short k-cycles over S^n of length m is given by*

$$\#\mathrm{C}_m^L(n, \ell, k) = \sum_{i=1}^{k} \sum_{j=0}^{q_m - 1} \frac{(L-1)^{q_m}}{q_m - j} \binom{m-1}{q_m - 1 - j} \binom{mk - im}{j} - \sum_{d \in D_m^L(n,\ell,k)} \frac{d}{m} \#\mathrm{C}_d^L(n, \ell, k). \tag{5.4}$$

The proofs of Theorem 5.2 and Theorem 5.3 use the same techiniques as the proofs of their Boolean counterpart. Thus, we decided to omit them.

6. Concluding remarks

We characterized a family of generators for short k-cycles over any Galois field. We used these generators to provide a recursive formula for for the number of short k-cycles in n variables of degree ℓ that have length m, where m is a divisor of n/k such that $n/(km)$ divides ℓ. We hope and expect to see applications of our results.

Acknowledgments. The research of the second author was supported by UPR-FIPI 7240022.00 and by The Puerto Rico Science, Technology and Research Trust (PRST) under agreement number 2020-00124. This content is only the responsibility of the authors and does not necessarily represent the official views of The Puerto Rico Science, Technology and Research Trust. The first author was supported as a student by PRST 2020-00124. The third author was supported as a student by UPR-FIPI 7240022.00.

References

[1] J. Cai, F. Green, and T. Thierauf. On the correlation of symmetric functions. *Math. Systems Theory* 29 (1996) 245–258.
[2] C. Carlet. Boolean functions for cryptography and error correcting codes, in: Boolean Methods and Models. *Cambridge University Press*, Cambridge (2010) 257– 397.
[3] F. Castro, R. Chapman, L.A. Medina, L. B. Sepúlveda Recursions associated to traprezoid, symmetric and rotation symmetric functions over Galois fields. *Discrete Math.* 314 (2018)1915–1931.
[4] F. Castro, O. E. González and L. A. Medina. Diophantine equations with binomial coefficients and perturbations of symmetric Boolean functions. *IEEE Trans. Inform. Theory* 64(2) (2018) 1347–1360.
[5] F. Castro and L. A. Medina. Linear Recurrences and Asymptotic Behavior of Exponential Sums of Symmetric Boolean Functions. *Elec. J. Combin.* 18 (2011), #P8.
[6] F. Castro and L. A. Medina. Asymptotic Behavior of Perturbations of Symmetric Functions. *Annals of Combin.* 18 (2014) 397–417.
[7] F. Castro, L. A. Medina, P. P. Stănică. Generalized Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent. *Appl. Algebra Eng. Commun. Comput.* 29 (2018) 1–21.
[8] F. Castro, L. A. Medina, L. B. Sepúlveda Closed formulas for exponential sums of symmetric polynomials over Galois fields. *J. Algebr. Comb.* 50 (2019) 73–98.
[9] T. W. Cusick. Weight recursions for any rotation symmetric Boolean functions. *IEEE Trans. Inf. Theory* 64(4) (2018) 2962–2968.
[10] T. W. Cusick and Y. Cheon. Theory of 3-rotation symmetric cubic Boolean functions. *J. Math, Cryptol.* 9(1) (2015) 45–62.
[11] T. W. Cusick and Y. Cheon. Weights for short quartic Boolean functions. *Inf. Sci.* 547 (2021) 18–27.
[12] T. W. Cusick, Y. Cheon and K. Dougan. Equivalence of 2-rotation symmetric quartic Boolean functions. *Inf. Sci.* 508 (2020) 358–379.
[13] T. W. Cusick and B. Johns. Recursion orders for weights of Boolean cubic rotation symmetric functions. *Discr. Appl. Math.* 186 (2015) 1–6.

[14] T. W. Cusick and B. Johns. Theory of 2-rotation symmetric cubic Boolean functions. *Des. Codes Cryptogr.* 76 (2015) 113–133.
[15] T. W. Cusick and Y. Li. k-th order symmetric SAC Boolean functions and bisecting binomial coefficients. *Discrete Appl. Math.* 149 (2005) 73–86.
[16] T. W. Cusick, Y. Li, and P. Stănică. Balanced Symmetric Functions over $GF(p)$. *IEEE Trans. Inf. Theory* 5 (2008) 1304–1307.
[17] T. W. Cusick and P. Stănică. Fast evaluation, weights and nonlinearity of rotation symmetric functions. *Discr. Math.* 258 (2002) 289–301.
[18] T. W. Cusick, P. Stănică. Cryptographic Boolean Functions and Applications *Academic Press*,(Ed. 2), San Diego, CA, 2017.
[19] D. K. Dalai, S. Maitra, and S. Sarkar. Results on rotation symmetric bent functions. *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06*, publications of the universities of Rouen and Havre (2006) 137–156.
[20] M. Hell, A. Maximov, and S. Maitra. On efficient implementation of search strategy for rotation symmetric Boolean functions. *Ninth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2004*, Black Sea Coast, Bulgaria, 2004.
[21] S. Kavut and D. Yücel. 9-variable Boolean functions with nonlinearity 242 in the generalized rotaiton symmetric class. *Information and Computation* 204(4) (2010) 341–350.
[22] P. V. Kumar, R. A. Scholtz and L. R. Welch. Generalized bent functions and their properties. *J. Combin Theory -Ser. A* 40 (1985) 90–107.
[23] Y. Li and T.W. Cusick. Linear Structures of Symmetric Functions over Finite Fields. Inf. Processing Letters 97 (2006) 124–127.
[24] Y. Li and T. W. Cusick. Strict Avalanche Criterion Over Finite Fields. *J. Math. Cryptology* 1(1) (2007) 65–78.
[25] M. Liu, P. Lu and G.L. Mullen. Correlation-Immune Functions over Finite Fields. *IEEE Trans. Inf. Theory* 44 (1998), 1273–1276.
[26] J. Pieprzyk and C.X. Qu. Fast hashing and rotation-symmetric functions. *J. Universal Comput. Sci.* 5(1) (1999) 20–31.
[27] P. Stănică, S. Maitra. Rotation symmetric Boolean functions—Count and cryptographic properties. *Discr. Appl. Math.* 156(10) (2008) 1567–1580.

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
Email address: joseemilio.calderon@upr.edu

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
Email address: luis.medina17@upr.edu

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
Email address: carlos.molina2@upr.edu