Discrete Mathematics 341 (2018) 3271–3280

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the matrix of rotation symmetric Boolean functions

Lavinia C. Ciungu, Miodrag C. Iovanov *

Department of Mathematics, University of Iowa, 14 MacLean Hall, Iowa City, IA 52242, United States

ARTICLE INFO

Article history:
Received 7 December 2016
Received in revised form 27 February 2018
Accepted 16 April 2018

Keywords:
Cryptography
Boolean function
Hamming weight
Rotation symmetry
RSBF
Group representations
Representation theory

ABSTRACT

In the study of rotation symmetric Boolean functions (RSBFs), it is natural to consider the equivalence of Boolean vectors in $\mathbb{F}_2^n$ given by $v \sim w$ if w is obtained from v by cyclic permutation (rotation). Several authors (Clark, Cusick, Hell, Maitra, Maximov, Stănică), in relation to RSBFs, considered the square matrix ${}_n\mathcal{A}$ obtained as follows: let $(G_i)_{i=1,\dots,g_n}$ be the equivalence classes of this relation $\sim$ and Λ_i be representatives; the entries of ${}_n\mathcal{A}$ are $(\sum_{x\in G_i}(-1)^{x\cdot\Lambda_j})_{i,j}$. Some properties of this matrix were obtained for n odd in the literature. We obtain a few new formulas regarding the number of classes of various types, and investigate the matrix ${}_n\mathcal{A}$ in general. One of our main results is that ${}_nA$ satisfies $({}_nA)^2 = 2^n\mathrm{Id}$, and it is conjugate to its transpose by a diagonal matrix. This is not an immediate consequence of the similar property of the related Hadamard type matrix $(p_{v,w})_{v,w\in\mathbb{F}_2^n} = ((-1)^{v\cdot w})_{v,w}$, but it is rather connected to character theory. We show that the entries of the matrix ${}_n\mathcal{A}$ are essentially the character values of the irreducible representations of the semidirect (or wreath) product of $\mathbb{F}_2^n \rtimes C_n$, where C_n is the cyclic group with n elements, which yields further properties of this matrix. This connection suggests possible future investigations, and motivates the introduction of Boolean functions with various other types of symmetry.

1. Introduction

Boolean functions are fundamental and have many applications in Coding Theory and Cryptography; we refer to the monograph [6] for a detailed account of Boolean functions. Rotation symmetric Boolean functions (RSBFs) seem to have been introduced independently by Filiol and Fountaine [8] and by Pieprzyk and Qu as components in rounds of a hashing algorithm [11]. This property is very important for fast and efficient computations in certain algorithms involving Boolean functions, and it proved useful in several areas of cryptography. There has been a lot of interest in various aspects of RSMF's in the last 15 years — see [1,3–5,9,13–15] and references therein. A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (or more generally, a function $f : \mathbb{F}_2^n \to \mathbb{C}$) is rotation symmetric if $f(x_1, \dots, x_n) = f(x_2, \dots, x_n, x_1)$, i.e. the values of f remain invariant under cyclic permutations of the entries in the input $(x_1, \dots, x_n)$. Following notation of [10,13,14], one is naturally led to partition $\mathbb{F}_2^n$ into subsets $G_{n,i}$, each consisting of all cyclic permutations of a single vector v in $\mathbb{F}_2^n$. These are equivalence classes of the equivalence relation $\sim$ given by $v \sim w$ if w is obtained from v by cyclic permutation (rotation), or equivalently, $G_{n,i}$ are orbits of the natural action of the cyclic group C_n on $\mathbb{F}_2^n$ by rotation (cyclic permutation of factors).[1] Let g_n be the number of such orbits $G_{n,i}$, and let $\Lambda_{n,i} \in G_{n,i}$ be representatives. The following matrix becomes important in the study of such rotation

* Corresponding author.
E-mail addresses: lavinia-ciungu@uiowa.edu (L.C. Ciungu), miodrag-iovanov@uiowa.edu (M.C. Iovanov).

[1] Some authors use the word "groups" when referring to $G_{n,i}$; we will use the term orbits, since we are also dealing with groups in the algebraic meaning of the term.

https://doi.org/10.1016/j.disc.2018.04.019
0012-365X/

symmetric Boolean functions and is considered by several authors (see for example [14,10,13] and references therein)

$$_n\mathcal{A} = (\sum_{x\in G_{n,i}} (-1)^{x\cdot A_{n,j}})_{i,j}$$

where $(v_1, \ldots, v_n)\cdot(w_1, \ldots, w_n) = v_1w_1 + \cdots + v_nw_n$ for $(v_1, \ldots, v_n), (w_1, \ldots, w_n) \in \mathbb{F}_2^n$. It is shown in [10] that for n odd, the number of orbits of even weight and the number of orbits of odd weight are equal, and in this case, after a suitable permutation of $\{1, \ldots, g_n\}$, a nice 2×2 block decomposition of this matrix with blocks of size $g_n/2$ is given there. Other formulas for the number of various types of orbits are given in [13]; see also [9,4,14]. Our goal is to investigate and give properties of this matrix in general. Such properties turn out to yield general identities between the elements of this matrix.

We investigate properties of the number g_n and prove it is always even. We give a general formula for the number h_n of orbits with even weight for arbitrary n, extending results of [10] (where such results were obtained for n odd). We also find formulas for the number of orbits of other types.

We then investigate algebraic properties of the matrix $_n\mathcal{A} = (a_{i,j})_{i,j}$. We first note that the entries of the matrix satisfy a property of the type $a_{j,i} = \frac{d_j}{d_i}a_{i,j}$, where $d_i = |G_{n,i}|$ is the number of elements of $G_{n,i}$. This shows that $_n\mathcal{A}$ is "close" to being symmetric: more precisely, it is conjugate to its transpose by a *diagonal* matrix with certain particular entries on the diagonal (which are positive integers).

Since the definition of this matrix $_n\mathcal{A}$ is closely related to the characters of $\mathbb{F}_2^n$, Fourier–Walsh theory and the action by rotation of the cyclic group with n elements C_n on $\mathbb{F}_2^n$, it is natural to try to relate this matrix with character theory of $\mathbb{F}_2^n$ and of the resulting semidirect product $\mathbb{F}_2^n \rtimes C_n$. In our main result, we prove the following fact (Theorem 3.8): the square of this matrix is a multiple of the identity

$$(_n\mathcal{A})^2 = 2^n \cdot \mathrm{Id}_{g_n} \tag{1}$$

While perhaps this may not seem surprising at first, since it is easy to see that the related $2^n \times 2^n$ matrix $P = ((-1)^{x\cdot y})_{x,y\in\mathbb{F}_2^n}$ has the similar property $P^2 = 2^n\mathrm{Id}_{2^n}$ (but different size $2^n \neq g_n$), Eq. (1) does not follow from this directly, but rather, it is more closely related to the properties of the semidirect product $\mathbb{F}_2^n \rtimes C_n$ (which is also a wreath product), and its representation theory. Indeed, the other main observation of this note is the following: on one hand, we show that the entries of $_n\mathcal{A}$ are values in the character table of $\mathbb{F}_2^n \rtimes C_n$, and on the other hand, all the values in this character table are "close" to being entries of $_n\mathcal{A}$: they all equal some entry of $_n\mathcal{A}$ times a corresponding complex root of unity or zero.

We give two proofs of the above relation, one which is direct and will be of interest to the general reader, and one based on the orthogonality of characters of $\mathbb{F}_2^n \rtimes C_n$. The direct proof is elementary and can be rewritten without any reference to Fourier–Walsh and character theory of $\mathbb{F}_2^n$, but it is nonetheless more transparent when formulated in such terms. On the other hand, the second (representation theoretic) approach yields a series of new formulas involving the elements of $_n\mathcal{A}$ in addition to the above information contained in Eq. (1) (Proposition 4.1). While one may likely again be able to prove these directly, it is more difficult to "guess" such relations a priori.

We note that many properties of RSBFs (balanced, bent, m-resilient) can be expressed in terms of multiplication of certain vectors by the matrix $_n\mathcal{A}$ (see [14, Proposition 1 and Lemma 2]), and hence the formula (1) becomes relevant. Therefore, we believe that the above mentioned representation theoretic connection – which seems to have not been explored so far – is worth mentioning, as it may likely have further implications on RSBFs and may be of use in future investigations. For example, the fusion rules (Clebsch–Gordon formulas) of $\mathbb{F}_2^n \rtimes C_n$ are closely related to various products of entries of the matrix $_n\mathcal{A}$.

Finally, we introduce Boolean functions which have symmetric invariance properties with respect to other groups G (such as Dihedral or linear) - which we call *G-invariant Boolean functions*. Given G a subgroup of the symmetric group of the set $\{1, \ldots, n\}$, we say that a Boolean function f of n-variables is G-invariant if $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for all $\sigma \in G$. We note that the matrix of G-invariant Boolean function A_G defined in a similar fashion with $_n\mathcal{A}$ satisfies the same property, which further emphasizes the representation theoretic connection of the result, and motivates the study of this relation. We suspect these G-invariant functions will share many of the important properties of RSBFs, while at the same time allowing for more freedom in the choice of group G for applications, and warrant further investigation.

2. Preliminaries

Let $\mathbb{V}_n = \mathbb{F}_2^n$ be the vector space of dimension n over the two-element field $\mathbb{F}_2$. For two vectors in $\mathbb{V}_n$, say $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$, we define the scalar product $a\cdot b = a_1b_1 + \cdots + a_nb_n$, where the multiplication and addition $+$(denoted by $\oplus$ in some sources and called *xor*) are over $\mathbb{F}_2$.

Definition 2.1. A *Boolean function* in n variables is a map from $\mathbb{V}_n$ to $\mathbb{F}_2$. The $(0, 1)-$ sequence defined by $(f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$ is called the *truth table* of the function, where $v_0 = (0, 0, \ldots, 0)$, $v_1 = (0, 0, \ldots, 1), \ldots, v_{2^n-1} = (1, 1, \ldots, 1)$ are usually ordered lexicographically.

Definition 2.2. The *Hamming weight* of a vector $x \in \mathbb{V}_n$, denoted by $wt(x)$, is the number of 1's in the vector x. A Boolean function is *balanced* if $wt(x) = 2^{n-1}$, that is the number of 0's equals the number of 1's in the truth table.

Many properties of Boolean functions can be described by the Walsh transform (or Walsh spectrum).