Truncated rotation symmetric Boolean functions Extended Abstract

Thomas W. Cusick[a] [*], Younhwan Cheon[b] [†]

[a]Department of Mathematics, University at Buffalo
244 Mathematics Bldg., Buffalo, NY 14260
[b]Department of Defence System Science, Korea Army Academy at YeongCheon
135-9, Hoguk-ro, Gogyeong-myeon, Yeongcheon-si, Gyeongsangbuk-do, Republic of Korea,38900

June 26, 2023

1 Introduction

Let $\mathbf{V}_n$ denote the set of all $n-$tuples $(x_1, \ldots, x_n)$ with entries in $GF(2)$ and let B_n denote the set of all Boolean functions g_n in n variables. We use $wt(g)$ for the (Hamming) weight of a Boolean function g and we say that any function in B_n is balanced if its weight is 2^{n-1}.

Definition 1. *Let ρ denote the cyclic shift defined on $\mathbf{V}_n$ by $\rho((x_1, \ldots, x_n)) = (x_2, \ldots, x_n, x_1)$. A function $g \in B_n$ is called rotation symmetric (RS) if and only if for any $(x_1, \cdots, x_n) \in \mathbf{V}_n$, $g(x_1, \cdots, x_n) = g(\rho^k(x_1, \cdots, x_n))$ for any $1 \leq k \leq n$. It is called monomial rotation symmetric (MRS) if it is generated by a single monomial.*

Rotation symmetric functions are important because of their applications in cryptography (see [10, Section 6.2], which has about 16 pages devoted to the history of the research on these functions), and more generally in some algorithms using Boolean functions whose efficient evaluation is necessary.

Any quadratic MRS function $g(x)$ in n variables can be written as

$$(1, j)_n = g_{n,j}(x) = x_1x_j + x_2x_{j+1} + \cdots + x_nx_{j-1} \tag{1}$$

[*] email: cusick@buffalo.edu

[†] email: yhcrypt@gmail.com

for some j with $2 \leq j \leq \lceil \frac{n+1}{2} \rceil$, or, in the special case when n is even and $j = \frac{n}{2} + 1$, as

$$g_{n,\frac{n}{2}+1}(x) = x_1 x_{\frac{n}{2}+1} + x_2 x_{\frac{n}{2}+2} + \cdots + x_{\frac{n}{2}} x_n. \tag{2}$$

These functions g_n are called *bent functions* and this is equivalent to saying $wt(g_n) = 2^{n-1} \pm 2^{(n/2)-1}$ (see [10, Def. 5.1, p. 84]).

Definition 2. *A modified MRS function $f \in B_n$ is called truncated rotation symmetric (TRS) if the function stops the expansion for the n-variable MRS function at the term where x_n first occurs.*

Thus any quadratic TRS function $f(x)$ in n variables can be written as

$$[1, j]_n = f_{n,j}(x) = x_1 x_j + x_2 x_{j+1} + \cdots + x_{n-j+1} x_n \tag{3}$$

for some j with $2 \leq j \leq \lceil \frac{n+1}{2} \rceil$.

For example, $(1, 2)_5 = g_{5,2}(x) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ and $[1, 2]_5 = f_{5,2}(x) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5$.

The TRS functions are important because they play an important role in the algorithm that enables the computation of linear recursion relations for the weights of any MRS or TRS function. The algorithm is explained in detail in [9] and a Mathematica program which performs the algorithm is given in [8]. It turns out that the recursion relations for any MRS function also apply to the corresponding TRS function (with different weights for the two functions), but it is much simpler to describe (and program) the algorithm for the TRS case. This was first observed, for degree 3 MRS functions only, in [2], but the generalization to arbitrary RS and TRS functions of any degree was not achieved until [8, 9]. There has been much work on various extensions and generalizations of this work since 2012, for instance [3, 4, 5, 11, 12].

It seemed for some time that the algorithm of [9] was not needed in the quadratic MRS case, since the work of [13] in 2009 already gave easy ways to directly compute the weight and nonlinearity for the functions $(1, j)_n$ in (1). However it was shown in [6, 7], using new ideas, that combining the algorithm with the results of [13] leads to very complete information about the weight and nonlinearity of the quadratic MRS functions, and also a complete determination of those n for which any function $(1, j)_n$ is balanced. The purpose of this paper is to obtain new results about the TRS functions $[1, j]_n$ in order to more fully understand the connections between those functions and the MRS functions. This paper shows that in some ways the TRS theory is more complicated than the MRS theory, but in other ways it is simpler. In particular we prove a precise formula for the generating function of the sequence of weights for the TRS functions which is simpler than the corresponding formula for the weights of the MRS functions. For details of the latter formula, see [7, Theorem 5.4].

2 Preliminaries

We shall also need the concept of *Walsh transform.* The Walsh transform of a function g in n variables is the map $W(g) : \mathbf{V}_n \rightarrow R$ defined for $w \in \mathbf{V}_n$ by

$$W(g)(w) = \sum_{x \in \mathbf{V}_n} (-1)^{g(x)+w \cdot x},$$

where the values of g are taken to be the real numbers 0 and 1. The integers $W(g)(w)$ are called *Walsh values.* We are especially interested in the Walsh values for $w = \mathbf{0} = (0, \ldots, 0)$ because of the well known [10, Lemma 2.10] fact

$$wt(g_n) = 2^{n-1} - \frac{1}{2} W(g_n)(\mathbf{0}). \tag{4}$$

We need the definition of a *plateaued* Boolean function (see [10, pp. 78-79] for some history). We say that a Boolean function function $g = g_n$ in n variables is *v-plateaued* if every Walsh value $W(g)(w)$ is either 0 or $\pm 2^{(n+v)/2}$ and we say that $v = v(n)$ is the v-value of g_n or that $v(n)$ is one of the v-values for g. It is well known that any quadratic Boolean function is plateaued. A discussion of v-values for ordinary RS quadratic functions is in [6, pp. 1310-1311] and a discussion for a much broader class of functions is in [1] (that paper uses s instead of our $v(n)$).

3 The v-values for quadratic TRS functions

In this section we find all of the v-values for the functions $[1, j]_n$ and we determine every element in the period for those values. Extending this work to other quadratic TRS functions seems to require new ideas. We first need the following lemma which gives the values of n for which $[1, j]_n$ is a bent function, and more.

Lemma 1. *The functions $f_{n,j} = [1, j]_n$ are bent, and in fact $W(f_{n,j})(\boldsymbol{0}) = 2^{n/2}$, for $n = (2j-2)k,\ k \geq 1$. The functions $f_{n,j}$ have $W(f_{n,j})(\boldsymbol{0}) = 2^{(n+j-1)/2}$ for $n = j - 1 + (2j-2)k,\ k \geq 1$.*

Theorem 1. *The sequence of the v-values for $f_{n,j} = [1,j]_n$, beginning at $n = 2j-2$, has initial entries $0, 1, 2, \ldots, j-2, j-1, j-2, j-3, \ldots, 2, 1$ and is periodic with period $2j-2$.*

Theorem 2. *The functions $f_n(x) = [1,j]_n$ are never balanced for $n \geq 2j-2$.*

We let $G(f)$ denote any closed formula for the generating function $gen(f)$ of f, where $gen(f) = \sum_{i=1}^{\infty} wt(f_n)x^{n-1}$. We shall only use this notation for truncated RS functions. The next theorem determines $G([1,t])$ for all $t \geq 2$.

Theorem 3. *For $f_n = [1,t]_n, t \geq 2$, We have*

$$G(f) = \frac{(\sum_{i=0}^{t-2} x^i)2^{t-2}x^{t-1}}{(1-2x)(1-2^{t-1}x^{2(t-1)})} = \frac{(1-x^{t-1})2^{t-2}x^{t-1}}{(1-x)(1-2x)(1-2^{t-1}x^{2(t-1)})}$$

The examples below include a sum of two TRS functions, though we cannot yet prove the extension of Theorem 3 to those cases. The obstacles include generalizing Theorem 1 and finding a formula for the numerator of the rational function $G(f)$ when f has more than one TRS function.

Example 1. *For $f_n = [1,2]_n$, we have*

$$G(f) = \frac{x}{(1-2x)(1-2x^2)}$$

$gen([1,2])(x) = x+2x^2+6x^3+12x^4+28x^5+56x^6+120x^7+240x^8+496x^9+\cdots$

Example 2. *For $f_n = [1,2]_n + [1,3]_n$, we have*

$$G(f) = \frac{4x^3(2-4x+5x^2-10x^3+8x^4)}{(1-2x)(1-2x+2x^2-4x^3+4x^4)}$$

$gen([1,2]+[1,3])(x) = 8x^3 + 16x^4 + 36x^5 + 72x^6 + 136x^7 + 272x^8 + 544x^9 + 1056x^{10} + 2080x^{11} + 4160x^{12} + 8256x^{13} + 16384x^{14} + \cdots$

References

[1] N. Anbar, W. Meidl and A. Topuzoglu, Idempotent and p-potent quadratic functions: distribution of nonlinearity and co-dimension, *Des. Codes Cryptogr.* 82 (2017), 265-291.

[2] A. Brown and T. W. Cusick, Recursive weights for some Boolean functions, *J. Math. Cryptol.* 6 (2012), 105-135.

[3] F. Castro, R. Chapman,L. Medina, L. Sepulveda and L. Brehsner, Recursions associated to trapezoid, symmetric and rotation symmetric functions over Galois fields, *Discrete Math.* 341 (2018), 1915–1931.

[4] F. Castro and L. Medina, Modular periodicity of exponential sums of symmetric Boolean functions, *Discrete Appl. Math* 217 (2017), 455-473.

[5] F. Castro, L. Medina and P. Stănică, Generalized Walsh transforms of symmetric and rotation symmetric boolean functions are linear recurrent, *Appl. Algebra Eng. Commun. Comput.* 29 (2018), 433-453.

[6] A. Chirvasitu and T. W. Cusick, Affine equivalence for quadratic rotation symmetric functions, *Des. Codes Cryptogr.* 88 (2020), 1301-1329.

[7] A. Chirvasitu and T. W. Cusick, Symbolic dynamics and rotation symmetric Boolean functions, *Cryptogr. Commun.* 14 (2022), 1091-1115.

[8] T. W. Cusick, Weight recursions for any rotation symmetric Boolean functions, https://arxiv.org/abs/1701.06648, 18 pp., 2017.

[9] T. W. Cusick, Weight recursions for any rotation symmetric Boolean functions, *IEEE Trans. Inform. Theory* 64 (2018), 2962-2968.

[10] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, second ed. (San Diego: Academic Press, 2017). First edition 2009.

[11] A. Gomez-Flores, L. Medina, L. Pomales and C. Santiago-Calderon, Recurrences in terms of special polynomials for exponential sums of elementary symmetric polynomials over finite fields, *Integers* 23 Paper No. A11, 17 pp., 2023.

[12] A. Gomez-Flores, L. Medina and P. Stănică, Recursions for modified Walsh transforms of some families of Boolean functions, *Rocky Mountain J. Math.* 52 (4) (2022), 1355-1373.

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