$$(1,2,4)_6 = 124 + 235 + 346 + 145 + 256 \ (n = 6 \ terms)$$

$$\text{Truncated RS function } Tr[(1,2,4)_6] = 124 + 235 + 346$$

$$\text{Extended truncated RS function } Ext[(1,2,4)_6] = 124 + 235 + 346 + 145$$

It was proved in [3, 4] that for any RS function f_n in n variables the sequence of weights $wt(f_n), n \geq \deg\ f$, satisfies a homogeneous linear recursion with integer coefficients. It was also proved that the associated recursion polynomial could be explicitly calculated as a divisor of the characteristic polynomial of a square *rules matrix* and an algorithm for computing the rules matrix was explained in [3]. A Mathematica program for computing the rules matrix was given in [4]. A recent paper (to appear) gives a simple method, using generating functions, for finding the sequence of weights $\{wt(f_n) : n \geq d\}$ for any Boolean function f of degree d in n variables, provided that the degree 2 ECC described below is true for degree d.

Easy Coefficients Conjecture For any quadratic RS Boolean function f_n of form $f_n = \sum_{i=1}^{k}(1, t(i))_n$, let $M = \max(t(i) - 1)$. Then the method of [3, 4] gives a nonsingular square rules matrix $R(f_n)$ of size $2^M + 1$. Let the roots of the minimal polynomial of this matrix be 2 and $\mu_i : 1 \leq i \leq 2^M$. Let the multiset $\eta_i,\ 1 \leq i \leq 2^M + 1$ consist of the roots μ_i, each repeated as often as its multiplicity in the characteristic polynomial of $R(T)$. Then

$$wt(f_n) = 2^{n-1} - \sum_{j=1}^{2^M} \frac{1}{2}\eta_j^n,\ n = 1, 2, \ldots \tag{1}$$

References

[1] A. Chirvasitu and T. W. Cusick, Affine equivalence for quadratic rotation symmetric Boolean functions, *Designs, Codes and Cryptography* **88** (2020), 1301-1329.

[2] A. Chirvasitu and T. W. Cusick, Symbolic dynamics and rotation symmetric Boolean functions, *Cryptography and Communications* **14** 2022, 1091-1115. Theorem 4.4 proves the ECC for monomial quadratic RS functions $(1, t)_n$.

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

[4] T. W. Cusick, Weight recursions for any rotation symmetric Boolean functions. arXiv:1701.06648 (2017).

1 A question about affine equivalence of quadratic RS functions

It is notoriously difficult to analyze general affine equivalence for Boolean functions, but the quadratic case is much easier because of the following well-known lemma ($N(f)$ = nonlinearity of f), which is true only for Boolean functions of degree 2.

Lemma 1. *Two quadratic functions f and g in n variables are affine equivalent if and only if $wt(f) = wt(g)$ and $N(f) = N(g)$.*

This lemma provides a simple test for whether any two quadratic functions are affine equivalent.

Using the lemma plus the work in [2], it is not difficult to count the number of affine equivalence classes for the monomial RS (MRS) functions $(1, t)_n$. If we let $\tau(n)$ denote the number of positive integer divisors of n, then we have [1, Th. 4.3]:

Theorem 1. *The number of affine equivalence classes for the quadratic MRS functions $(1, t)_n$, $n \geq 3$, is $\tau(n) - 1$.*

It can be shown [1] that all possible weights for a quadratic RS function in n variables are 2^{n-1} (balanced function) and $2^{n-1} \pm 2^j$, $(n/2) - 1 \leq j \leq n-2$. Thus the number of possibilities for the pair $(weight, nonlinearity)$ is severely restricted. Computation for small n shows that the smaller weights in the allowed range never seem to occur, which would further restrict the possibilities. Thus the following question can be asked:

Is it possible that every quadratic RS function in n variables is affine equivalent to a function of form $f_n = \sum_{i=1}^{[(n-1)/2]} (1, t(i))_n$, where the number of nonzero $t(i)$ is $\leq B$ for some fixed integer B? We have no example where even the very strong assertion with $B = 3$ is disproved.

References

[1] A. Chirvasitu and T. W. Cusick, Affine equivalence for quadratic rotation symmetric Boolean functions, *Designs, Codes and Cryptography* **88** (2020), 1301-1329.

[2] 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, pp. 428-432, 2009.

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 $W(g) : \mathbf{V}_n \to R$ 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.