Classes of Plateaued Rotation Symmetric Boolean Functions under Transformation of Walsh Spectra

Alexander Maximov

Department of Information Technology, Lund University
P.O. Box 118, 221 00 Lund, Sweden
movax@it.lth.se

Abstract. Construction methods of Boolean functions with cryptographically significant properties is an important and difficult problem. In this work we investigate the class of rotation symmetric Boolean functions (RSBFs). These functions are invariant under circular translation of indices and were mainly introduced for efficient implementation purposes. First, we derive general results on these functions. Afterwards, we concentrate on plateaued RSBFs on odd number of variables, which have three valued Walsh Spectra $(0, \pm\lambda)$, and can have maximum nonlinearity. We consider both cases when the number of variables n is composite and prime. When n is odd and prime, we derive the constructive relation between *balanced/unbalanced* plateaued RSBFs and show how from one given such function the complete sub class can be generated. As long as search for one plateaued RSBF is of high complexity, our proposed manipulation technique with Walsh spectra imediately give us the way to construct many such functions without time consuming. Since the most important properties of a function are determined via the values of Walsh spectra, then such transformation technique is important to create new function with, possible, better properties. The application of our transformation technique construct a class of $\left((2^{\frac{n-1}{2}}+1)/n\right)! \cdot \left(2^{\frac{n-1}{2}}-1\right)$ balanced/unbalanced plateaued RSBFs. In our practical implementation of this technique, given one balanced PRSBF on $n = 11$ variables we could construct 185 new such functions. To find the first function took us several days, whereas to construct new 185 functions took us just a second. However, this technique can be applied only when the Legendre symbol $(2/n)$ is -1, and the first such n's are $3, 5, 7, 11, 13, 19, 29, 37, 43, \ldots$.

Keywords: algebraic attack, algebraic immunity, Boolean functions, plateaued functions, balancedness, nonlinearity, combinatorial cryptography, Walsh transform.

1 Introduction

A proper choice of a Boolean function as a nonlinear filter in design of a cipher is an important and difficult task for cryptography [1–3]. A bad choice of such a function is the bottleneck for correlation and algebraic attacks [4]. Therefore, methods for Boolean functions construction with good cryptographic properties always were the subject of significant attention in scientific cryptography (see [1–3] and the references in these papers).

At Eurocrypt 1998, a new class of functions was introduced [5], Rotation Symmetric Boolean Functions (RSBF), that are invariant under rotation of indices for its input variables. This subject met a lot of attention, and many results were achieved from that time. In 1998, Pieprzyk and Qu study RSBFs [6] as components in the round of a hashing algorithm, and found that RSBFs are useful when an efficient implementation is required. Other research on RSBFs continued in [7, 8, 1]. These functions appeared to be *efficient in implementation* [6, 8], *reach in terms of good cryptographic properties* [1, 5, 7, 9], *strong against of algebraic attacks* [4, 10], and *can be searched in an efficient way* [1, 11, 12].

1.1 Motivation to Study RSBFs

There are several reasons of why we need to study these functions, and we give them in this subsection.

1) *When efficient evaluation of a function is important*, for instance, in the implementation of MD4, MD5 or HAVAL ciphers, the properties of RSBFs are desirable, since one can reuse evaluation from previous iterations. It turns out that, for example, a degree 2 RSBF on n variables takes only $\frac{3n-1}{2} + 6(m-1)$ operations (additions and multiplications) to evaluate in m consecutive rounds of a hashing algorithm. One can simply consider the Feistel structure [1] [15, 16] of a hashing algorithm as a sequence of iterations where each iteration takes some input $X = (X_k, \ldots, X_0)$ and a message block M, and produce the output $Y = (Y_k, \ldots, Y_0)$ using the rule $Y = M + F(X_{k-1}, \ldots, X_0) + RSBF(X_k, s)$. Note that M, X_i, Y_i are blocks of N-bits, and $RSBF(X_k, s)$ is the circular rotation of the block X_k by s positions to the left, and F is another cryptographic primitive. Therefore, the study of the component $RSBF(X_k, s)$ of such hashing algorithms is important.
2) At [1, 5, 7, 9, 10], it has been shown that many functions in this class *are rich in terms of good cryptographic properties*. Furthermore, the RSBF class is much smaller ($\approx 2^{\frac{2^n}{n}}$) comparing to the space of n-variable Boolean functions (2^{2^n}) and, hence, *search techniques can be much more efficient*.
3) At Eurocrypt 2004, it has been shown [4] that a function f resists against algebraic attacks if the minimum degree for its annihilator h is large. In the same work the authors suggested to consider a new property of Boolean functions – *algebraic immunity* $AI(f)$, which is the minimum degree of a nonzero annihilator for the function f, characterizing its strength against of algebraic attacks. Later on, another group of researches in [10] showed that *RSBFs are rich of functions that are strong against of algebraic attacks.* They considered RSBFs with maximum nonlinearity and correlation immunity. For example, they found 12 RSBFs (7, 2, 4, 56) for which $AI(f) = 4$ – the maximum possible; there are 6976 RSBFs (8, 1, 6, 116) with the highest $AI(f) = 4$; there are *all* 8406 RSBFs [9, 3, 5, 240] with the highest $AI(f) = 4$ (there are no balanced (9, 3, 5, 240) RSBFs [11, 12], and, according to Corollary 1 (item 1) in [10], for such functions $AI(f)$ is strictly less then 5). From these work we see that the class of RSBFs contains many functions, which are strong against of algebraic attacks.
4) When the number of variables is *odd*, then we concentrate on *plateaued* RSBFs because of the following reasons. In [10] the authors show that $AI(f)$ is maximum only when f is balanced (for odd n) and have maximum nonlinearity. From one hand, given a Boolean function on an even number of input variables, the best possible nonlinearity can be achieved when the magnitudes of all the Walsh spectra values are the same. However, this is not possible when the number of input variables is odd. In such a scenario, the functions with three valued Walsh spectra $0, \pm\lambda$, which are known as *plateaued functions*, may be investigated [17, 18].

Summarizing the previous, we believe that the property of rotation symmetry is a good property, because it gives us many positive reflections. However, this property could probably leak information in some way, but nobody could find it so far. All this motivate us to investigate this class of functions in detail.

1.2 Preliminaries: Definitions and Notations

A Boolean function (BF) on n variables is a mapping $\{0,1\}^n \to \{0,1\}$, and can be defined by its *truth table*: $f = [f(0,0,\ldots,0), f(1,0,\ldots,0), f(0,1,\ldots,0), \ldots, f(1,1,\ldots,1)]$. A BF f is *balanced* if its truth table contains an equal number of 1's and 0's. Any BF has an unique representation as a polynomial over F_2, called the *algebraic normal form* (ANF),

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{1 \le i \le n} a_i x_i \oplus \bigoplus_{1 \le i < j \le n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0,1\}$. The *algebraic degree*, $\deg(f)$, is the number of variables in the highest order term with non-zero coefficient.

[1] Feistel structures are considered to be strong against different types of attacks, and it was used in such well-known ciphers as A5/3 [13] (a new encryption standard for mobile communication which was recently accepted), MUGI [14], and other ciphers.

Many properties of BFs can be described by the *Walsh transform* (WT). Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belong to $\{0,1\}^n$ and $x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n$. Let $f(x)$ be a BF on n variables. Then the *Walsh transform* of $f(x)$ is a real valued function over $\{0,1\}^n$, defined as

$$W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot \omega}.$$

The vector $[W_f(00\ldots0)\ldots W_f(11\ldots1)]$ is called *Walsh spectra* (WS). A Boolean function f is balanced iff $W_f(0) = 0$. The nonlinearity of f is given by $nl(f) = 2^{n-1} - \frac{1}{2}\max_{\omega \in \{0,1\}^n} |W_f(\omega)|$. A function is m-resilient (respectively mth order correlation immune) iff its Walsh spectra satisfies $W_f(\omega) = 0,$ for $0 \le w_{\mathrm{H}}(\omega) \le m$ (respectively $1 \le w_{\mathrm{H}}(\omega) \le m$).

Following the notation in [1–3] we use (n, m, d, σ) to denote an n-variable, m-resilient BF with degree d and nonlinearity σ. By $[n, m, d, \sigma]$ we denote an unbalanced n-variable, mth order correlation immune BF with degree d and nonlinearity σ.

1.3 Introduction to Plateaued RSBFs and Previous Work

Let $x_i \in \{0,1\}$ for $1 \le i \le n$. For $1 \le k \le n$, we define the permutation $\rho_n^k(x_i)$ as $\rho_n^k(x_i) = x_{i+k \bmod n}$. Let $(x_1, x_2, \ldots, x_{n-1}, x_n) \in \{0,1\}^n$. Then we extend the definition as $\rho_n^k(x_1, x_2, \ldots, x_{n-1}, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_{n-1}), \rho_n^k(x_n))$. I.e., ρ_n^k is a k cyclic rotation on an n-bit vector.

Definition 1. (RSBF) *A Boolean function f is called Rotation Symmetric if for each input $(x_1, \ldots, x_n) \in \{0,1\}^n$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$ for $1 \le k \le n$.*

The inputs to a RSBF can be divided into groups so that each consists of all cyclic shifts of one element. A *group of inputs* is generated by $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \le k \le n\}$. The number of the groups is denoted by g_n. Thus, the number of n-variable RSBFs is 2^{g_n}. A *group of inputs* can be represented by its *representative element* $\Lambda_{n,i}$ which is the lexicographically first element belonging to the group. The representative elements are again arranged lexicographically. *The rotation symmetric truth table* (RSTT) is defined as the g_n-bit string $[f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_{n-1}})]$. In [1] it was shown that Walsh transform takes the same value for all elements belonging to the same group, i.e., $W_f(u) = W_f(v)$ if $u \in G_n(v)$.

By Burnside's lemma [7] the number of groups is $g_n = \frac{1}{n}\sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}.$, where $\phi(k)$ is the Euler's *phi*-function. By $h_{n,w}$ we denote the number of groups of weight w, which can be recursively calculated as $(2^{g_{n,w}} - 1)2^{\sum_{i=0}^{w-1} g_{n,i}}$ [7].

For efficient work with RSBFs, the matrix ${}_n\mathcal{A}$ of size $g_n \times g_n$ were introduced [1]. The matrix ${}_n\mathcal{A}$ for an n variable RSBF is defined as

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

Using ${}_n\mathcal{A}$ matrix, the Walsh transform for an RSBF can be calculated from its RSTT as

$$W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n - 1} (-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,j}.$$

Recently, new results on RSBFs for *odd* number of variables n were received in [12]. Let us permute the rows and columns of ${}_n\mathcal{A}$ in the following way: the first $g_n/2$ rows and columns correspond to the representative elements $\Lambda_{n,i}$ of *even* weight, and the second $g_n/2$ rows and columns correspond to their complements. Then the new matrix, denoted as ${}_n\mathcal{A}^\pi$, has a nice structure:

$${}_n\mathcal{A}^\pi = \left(\begin{array}{c|c} {}_n\mathcal{H} & {}_n\mathcal{H} \\ \hline {}_n\mathcal{H} & -{}_n\mathcal{H} \end{array}\right).$$

Example: Let $n = 5$ – odd, for which $g_n = 8$. In [1], the group representatives $\Lambda_{n,i}$ are ordered lexicographically, i.e., $(0,0,0,0,0)$, $(0,0,0,0,1)$, $(0,0,0,1,1)$, $(0,0,1,0,1)$, $(0,0,1,1,1)$, $(0,1,0,1,1)$, $(0,1,1,1,1)$, $(1,1,1,1,1)$. For ${}_5\mathcal{A}^\pi$ the order is $(0,0,0,0,0)$, $(0,0,0,1,1)$, $(0,0,1,0,1)$, $(0,1,1,1,1)$, $(1,1,1,1,1)$, $(0,0,1,1,1)$, $(0,1,0,1,1)$, $(0,0,0,0,1)$. The new matrix ${}_5\mathcal{A}^\pi$ is of a nice sub matrix structure:

$$ {}_5\mathcal{A} = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 3 & 1 & 1 & -1 & -1 & -3 & -5 \\ 5 & 1 & 1 & -3 & 1 & -3 & 1 & 5 \\ 5 & 1 & -3 & 1 & -3 & 1 & 1 & 5 \\ \hline 5 & -1 & 1 & -3 & -1 & 3 & 1 & -5 \\ 5 & -1 & -3 & 1 & 3 & -1 & 1 & -5 \\ 5 & -3 & 1 & 1 & 1 & 1 & -3 & 5 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \end{array}\right), \; {}_5\mathcal{A}^\pi = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 1 & -3 & 1 & 5 & 1 & -3 & 1 \\ 5 & -3 & 1 & 1 & 5 & -3 & 1 & 1 \\ 5 & 1 & 1 & -3 & 5 & 1 & 1 & -3 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 5 & 1 & -3 & 1 & -5 & -1 & 3 & -1 \\ 5 & -3 & 1 & 1 & -5 & 3 & -1 & -1 \\ 5 & 1 & 1 & -3 & -5 & -1 & -1 & 3 \end{array}\right). \tag{1} $$

The existence of ${}_n\mathcal{H}$-submatrix for odd n follows from the property that

$$ {}_n\mathcal{A}^\pi_{r,c} = {}_n\mathcal{A}^\pi_{r,c+\frac{g_n}{2}} = {}_n\mathcal{A}^\pi_{r+\frac{g_n}{2},c} = -\,{}_n\mathcal{A}^\pi_{r+\frac{g_n}{2},c+\frac{g_n}{2}}, \quad \text{for } c,r = 0,1,\ldots,\tfrac{g_n}{2}-1. $$

Now, for notation purposes let us split the RSTT into two parts, σ_1 and σ_2, such that RSTT $= \sigma_1 \parallel \sigma_2 \in \{0,1\}^{g_n}$, and each $\sigma_1, \sigma_2 \in \{0,1\}^{g_n/2}$. Let us define a one-to-one mapping function

$$ \mu_\sigma : \sigma_1 \parallel \sigma_2 \in \{0,1\}^{\frac{g_n}{2}} \times \{0,1\}^{\frac{g_n}{2}} \longrightarrow \sigma_1^* \parallel \sigma_2^* \in \{\pm 1\}^{\frac{g_n}{2}} \times \{\pm 1\}^{\frac{g_n}{2}}, $$

such that, if $\sigma_{1_i} = 0$ then $\sigma^*_{1_i} = (-1)^0 = +1$, otherwise $\sigma^*_{1_i} = (-1)^1 = -1$. Then the Walsh transform for any input $\omega = (00\ldots0), \ldots, (11\ldots1)$ is calculated as:

$$ W_f(\omega) = ((\sigma_1^*\ {}_n\mathcal{H} + \sigma_2^*\ {}_n\mathcal{H}) \parallel (\sigma_1^*\ {}_n\mathcal{H} - \sigma_2^*\ {}_n\mathcal{H}))[\omega]. \tag{2} $$

In this paper we refer $w_1 = \sigma_1^*\ {}_n\mathcal{H}$ and $w_2 = \sigma_2^*\ {}_n\mathcal{H}$ as *partial Walsh Spectra*, or just *pWS*.

Definition 2. (PRSBF) *A Boolean function f is called plateaued if its Walsh spectra is 3-valued $\{0, \pm\lambda\}$ for any input in (2), where λ is called the amplitude of the function.*

According to (2), the Walsh transform in each position $\omega = i$ is 3-valued for PRSBFs, i.e.:

$$ w_{1_i} + w_{2_i} = 0 \text{ or } \pm\lambda, \qquad w_{1_i} - w_{2_i} = 0 \text{ or } \pm\lambda. \tag{3} $$

1.4 Our Contribution

The contribution of this paper can be divided into two general parts:

1) *Theoretical results on RSBFs.* First, for any n we derive the combinatorial result in a general case, $\eta_{n,t,w}$ – the number of groups of size t with elements of weight w. Sub cases of this formula were calculated in [7] ($h_{n,w}$ and g_n), and [12] ($d_{n,t}$), and was used to prove other results. This the most general nonrecursive formula is now proposed and also used to prove our results.
Second, we study plateaued RSBFs and the matrix ${}_n\mathcal{A}$. Our goal is to give an answer whether we theoretically can find functions with good properties or not, in this class. For this specific purpose, we consider appropriately chosen pair of columns and give an answer how many functions in this class lead to a "good" Walsh spectra at the corresponding points.
In the previous work [12] in order to prove the nonexistence of (9, 3, 5, 240), the authors intuitively considered the same two columns for the fixed matrix ${}_9\mathcal{A}$, and proved the nonexistence. However, their solution was for one specific case, and our contribution in this paper is the general nonexistence criteria when n is *odd composite*. Additionally, as an example, we give the proof of nonexistence of PRSBFs with maximum nonlinearity values such as (9, 3, –, –) with $\lambda = 32$, (15, 5, –, –) with $\lambda = 256$, and (21, 7, –, –) with $\lambda = 2048$. Although, we say that the function (15, 3, –, –) with $\lambda = 256$ falls our test and, hence, *could exist*. It means that at least for $n = 9, 15, 21$ there is no maximum resilient PRSBF with maximum amplitude and nonlinearity.

2) *Classes of plateaued RSBFs under transformation of Walsh spectra on n odd prime number of variables.* In the first part we considered when n is a composite number, whereas in the second part we investigate the case when n is *odd* and *prime*. During our work with Walsh spectra we found two observations on the structure of the matrix ${}_n\mathcal{A}$. This matrix can be permuted in a nice way so that it becomes to be in a compact representation. Finally, we found the way how to use these observations to derive two simple operations on the truth table of the function (basically, (a) swapping parts of RSTT and (b) local shifting), which result with the permutation of the Walsh spectra values, remaining the function to be balanced (unbalanced) plateaued RSBF. These transformations can permute Walsh spectra (WS) such that, for example, the resiliency can be increased, since zeros of WS can be "moved" to proper positions. However, we show that this technique can be applied only when the Legendre symbol $(2/n)$ is -1. The first such n's are $3, 5, 7, 11, 13, 19, 29, 37, 43, \ldots$. We say: *"Give us just one balanced plateaued RSBF on 43 variables, and we give you* $48771! \cdot 2097151$ *RSTT transformations back (some of the functions can be equal to each other depending on the structure of the given initial function)".*
In our simulations we could find (basically, by luck) a 0-resilient PRSBF on $n = 11$ variables, and then we could construct a 2-resilient function, using our technique.
Since we could not prove the observations, we decided to divide this approach in two sections. In Section 3 we describe our observations, and in Section 4 we give the method and the results which we could prove.

In this paper we in majority study functions on odd number of variables n. It has appeared that a parallel group of researches studied RSBFs on even n [19], and they concentrated on searching for Bent functions (these functions exist only when n is odd).

2 Our Theoretical Results on RSBFs

In this section we give combinatorial results on RSBFs. First, we start with a technical result that counts $\eta_{n,t,w}$ — the number of groups which contain exactly t elements of weight w. We note that all elements in a group have the same weight. In [7] the formula for $h_{n,w}$ – the number of long cycles groups with elements of weight w was studied in detail, and it appears to be a sub case of our generalized formula (see Corollary 1(e)).

Lemma 1. *For an n-variable RSBF the number of groups with t elements of weight w is*

$$\eta_{n,t,w} = \begin{cases} \frac{1}{t} \sum\limits_{\substack{k \mid t \\ q_k \mid w}} \mu(t/k) \cdot \binom{n/q_k}{w/q_k}, & \text{for } t, w = 1, \ldots, n, \text{ where } q_k = \frac{n}{\gcd(n,k)} \\ 1, & \text{for } t = 1,\ w = 0 \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where $\mu(t)$ is the Möbius function [20]*, i.e., $\mu(t) = 1$, if $t = 1$; $\mu(t) = 0$, if $e_i \geq 2$; and $\mu(t) = (-1)^m$, otherwise, when $t = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$ is factorized into powers of m distinct primes, $p_1, p_2 \ldots p_m$.*
Proof:

Let $S = \{0,1\}^n$ and let $x \in S$. Let $p_{t,w}$ be the number of elements from the set S of weight w such that $\rho_n^t(x) = x$. The number of orbits for these permutors is $\gcd(n,t)$, and to fulfill the requirement $\rho_n^t(x) = x$ each orbit must contain all 0's or all 1's. The number of elements in each orbit is $\frac{n}{\gcd(n,t)}$ and, to have the weight w, we also want that $\frac{n}{\gcd(n,t)} | w$. Then the number of orbits that will be filled with 1's is $\frac{w}{n/\gcd(n,t)}$, that can be placed in $p_{t,w} = \binom{gcd(n,t)}{\frac{w}{n/\gcd(n,t)}}$ ways. If we define $q_t = \frac{n}{\gcd(n,t)}$, then this binomial coefficient is then written as $p_{t,w} = \binom{n/q_t}{w/q_t}$. Now,

the recursive formula is:

$$\begin{cases} \eta_{n,1,0} = 1 \\ \eta_{n,t,w} = \frac{1}{t}(p_{t,w} - \sum\limits_{\substack{k|t \\ k<t \\ q_k|w}} k \cdot \eta_{n,k,w}) \end{cases} \quad \Rightarrow \quad \sum_{\substack{k|t \\ q_k|w}} k \cdot d_{n,k,w} = p_{t,w} = \binom{n/q_t}{w/q_t},$$

where $t, w = 1, \ldots, n$. We use the Möbius function [20] to invert the expression: $\eta_{n,t,w} = \frac{1}{t} \sum_{\substack{k|t \\ q_k|w}} \mu(t/k) \cdot \binom{n/q_k}{w/q_k}$, from which the proof follows. □

Corollary 1. *We can explicitly derive the following nonrecursive formulas:*

(a) The number of groups with t elements is $d_{n,t} = \sum_{w=0}^{n} \eta_{n,t,w} = \frac{1}{t} \sum_{k|t} \mu(t/k) 2^{\gcd(n,k)}$;
(b) The number of groups with elements of weight w is $g_{n,w} = \sum_{t=1}^{n} \eta_{n,t,w}$;
(c) The total number of groups is $g_n = \sum_{t=1}^{n} d_{n,t} = \sum_{t=1}^{n} \sum_{w=0}^{n} \eta_{n,t,w}$;
(d) The total number of elements is $|S| = \sum_{t=1}^{n} t \cdot d_{n,t} = \sum_{t=1}^{n} \sum_{w=0}^{n} t \cdot \eta_{n,t,w} = 2^n$;
(e) The number of groups of full cycle with elements of weight w is $h_{n,w} = \eta_{n,n,w}$;

□

The next question is whether a balanced plateaued RSBF with particular properties could exist or not. For this purpose we introduce the following notation. For a composite n and a prime number p such that $p|n$, let us define the following two representative elements:

$$\Lambda_0 = (\underbrace{00 \quad \ldots \quad 0}_{n}) \text{ and } \Lambda_p = (\underbrace{\underbrace{0\ldots01}_{p}\underbrace{0\ldots01}_{p}\ldots\underbrace{0\ldots01}_{p}}_{n/p}).$$

Note that Λ_p always contains an odd number of 1's, hence, in the matrix ${}_n\mathcal{H}$, the corresponding representative element for Λ_p is its complement $\bar{\Lambda}_p$. The idea is to consider two columns of the matrix ${}_n\mathcal{H}$ corresponding to Λ_0 and Λ_p – the columns which are responsible for balancedness of the function and for n/p-resiliency, respectively. We want to have a test whether the n/p-resilient function could exist or not by telling whether the Walsh spectra at these points can be 0 or not. We investigate these two columns jointly.

Lemma 2. *Let n be odd composite and p be a prime such that $p|n$ then ${}_n\mathcal{H}$ has the following properties:*

(i) the column corresponding to Λ_0 contains exactly $\frac{d_{n,t}}{2}$ values t;
(ii) if ${}_n\mathcal{H}_{i,\Lambda_0} = t$ then the value ${}_n\mathcal{H}_{i,\Lambda_p}$ must be of the form: ${}_n\mathcal{H}_{i,\Lambda_p} = t - \frac{4t}{p}r$, for some $r = [0 \ldots \frac{n-1}{2}]$. Obviously, if $\gcd(p,t) = 1 \Rightarrow r = 0$;
(iii) if ${}_n\mathcal{H}_{i,\Lambda_0} = t$ then the number of rows in ${}_n\mathcal{H}$ where ${}_n\mathcal{H}_{i,\Lambda_p} = t - \frac{4t}{p}r$ is:

$$\#(t, t - \frac{4t}{p}r) = \frac{1}{t}\binom{p}{2r} \sum_{k|t} \mu(t/k) \cdot q_k, \text{ where } q_k = \begin{cases} 2^{k-p}, & \text{if } \gcd(p,k) = p \\ 1, & \text{if } \gcd(p,k) = 1 \text{ and } r = 0 \\ 0, & \text{if } \gcd(p,k) = 1 \text{ and } r \neq 0. \end{cases} \quad (5)$$

Proof: see Appendix A1 □

Now we are ready to present the nonexistence criteria when n is odd and composite, and also give examples of applications of the test.

Theorem 1. (Nonexistence test for balanced PRSBFs on n odd composite)
For n odd and composite, let p be a prime number such that $p|n$. If there exists an (n/p)-resilient plateaued function with amplitude λ, then it must satisfy to the following test:

Consider columns of ${}_n\mathcal{H}$ corresponding to Λ_0 and Λ_p. Let the number of different pairs $({}_n\mathcal{H}_{i,\Lambda_0}, {}_n\mathcal{H}_{i,\Lambda_p})$ be m, and the pairs of values themselves are $(a_0, b_0), \ldots, (a_{m-1}, b_{m-1})$. Let $p_i =$

$\#\{(a_i, b_i)\}$ be the number of appearence of the corresponding pair (a_i, b_i) in the columns Λ_0 and Λ_p, calculated by the formula (5). Then, there must exist integers $k'_0, \ldots, k'_{m-1}$, $k''_0, \ldots, k''_{m-1}, k^*_i \in \{0 \ldots p_i\}$ ($k^*_i = k'_i$ or k''_i), such that: for some fixed $\tau_1 \in \{0, +1\}$ and $\tau_2 \in \{0, +1, -1\}$

$$\begin{cases} \sum_{i=0}^{m-1} a_i k'_i = \dfrac{\tau_1 \lambda + 2^n}{4}, \\ \sum_{i=0}^{m-1} a_i k''_i = \dfrac{-\tau_1 \lambda + 2^n}{4}, \end{cases} \quad \textit{and} \quad \begin{cases} \sum_{i=0}^{m-1} b_i k'_i = \dfrac{\tau_2 \lambda + 2\sum_{i=0}^{m-1} b_i p_i}{4}, \\ \sum_{i=0}^{m-1} b_i k''_i = \dfrac{\tau_2 \lambda + 2\sum_{i=0}^{m-1} b_i p_i}{4}. \end{cases} \tag{6}$$

Proof: see Appendix A2 □

In this theorem the first equation gives a condition for function balancedness, and the second equation performs a simple test that the function is (n/p)-resilient, since Λ_p column must give us Walsh spectra equal to 0, if the function is (n/p)-resilient. We have a hypothesis that $\sum_{i=0}^{m-1} b_i p_i$ is always 0. We also think that if a n/p-resilient plateaued RSBF exists, then τ_1 and τ_2 cannot be 0. The important question is to find the way to search the proper k^*_i's quickly, rather then to try them exhaustively.

The functions of significant interest are *balanced* plateaued functions with amplitude $\lambda = 2^{(n+1)/2}$ [2], because they have highest nonlinearity. We apply the nonexistence test to several such PRSBFs in the following examples.

Example: Consider $(9, 3, -, -)$ plateaued RSBF with $\lambda = 32$. To test whether such function could exist or not we use Theorem 1 above:

1. Choose $p = 3$ and test for $9/3 = 3$-resiliency. Determine the number of pairs (a_i, b_i), using Lemma 2. There are only $m = 4$ pairs: $(1, 1), (3, -1), (9, 9)$, and $(9, -3)$
2. We need to find the k^*'s. The conditions are the following:

i	(a_i, b_i)	$p_i = \#\{(a_i, b_i)\}$	range for k^*_i
0	(1, 1)	1	$k^*_0 \in [0 \ldots 1]$
1	(3, -1)	1	$k^*_1 \in [0 \ldots 1]$
2	(9, 9)	7	$k^*_2 \in [0 \ldots 7]$
3	(9, -3)	21	$k^*_3 \in [0 \ldots 21]$

$$\Rightarrow \begin{cases} 1k'_0 + 3k'_1 + 9k'_2 + 9k'_3 = (32\tau_1 + 512)/4 \\ 1k'_0 - 1k'_1 + 9k'_2 - 3k'_3 = (32\tau_2 + 0)/4 \\ 1k''_0 + 3k''_1 + 9k''_2 + 9k''_3 = (-32\tau_1 + 512)/4 \\ 1k''_0 - 1k''_1 + 9k''_2 - 3k''_3 = (32\tau_2 + 0)/4. \end{cases}$$

A simple search for $k^*_0, \ldots, k^*_3$ gives us the only two candidates for the half-functions σ's:

$$k_0 = 0, k_1 = 1, k_2 = 4, k_3 = 9, \text{ with } \tau_1 = -1 \text{ and } \tau_2 = +1$$

and the second is:

$$k_0 = 1, k_1 = 0, k_2 = 3, k_3 = 12, \text{ with } \tau_1 = +1 \text{ and } \tau_2 = -1.$$

It means that there is no pair of half-functions σ_* with (τ_1, τ_2) and $(-\tau_1, \tau_2)$. Hence, there is no 3-resilient plateaued functions on 9 variables.

□

We have applied the nonexistence criteria for several balanced plateaued RSBFs with $\lambda = 2^{\frac{n+1}{2}}$:

Case	Pairs	Possible candidates k_is									Existence
		$\tau_1 = -1$			$\tau_1 = 0$			$\tau_1 = +1$			
		$\tau_2 = -1$	$\tau_2 = 0$	$\tau_2 = +1$	$\tau_2 = -1$	$\tau_2 = 0$	$\tau_2 = +1$	$\tau_2 = -1$	$\tau_2 = 0$	$\tau_2 = +1$	
$n = 9, p = 3$	$\#(1,1) = 1$	-	-	0	-	-	-	1	-	-	Do
$\lambda = 32$	$\#(9,-3) = 21$			9				12			not
$(9, 3, -, -)$	$\#(9,9) = 7$			4				3			exist
	$\#(3,-1) = 1$			1				0			
$n = 15, p = 3$	$\#(1,1) = 1$	-	-	0	-	-	-	1	-	-	Do
$\lambda = 256$	$\#(15,-5) = 819$			403				416			not
$(15, 5, -, -)$	$\#(15,15) = 272$			138				134			exist
	$\#(5,5) = 3$			2				1			
	$\#(3,-1) = 1$			1				0			
$n = 15, p = 5$	$\#(1,1) = 1$	0	-	0	-	-	-	1	-	1	Could
$\lambda = 256$	$\#(15,3) = 682$	264		275				271		282	exist
$(15, 3, -, -)$	$\#(15,-9) = 341$	209		198				211		200	
	$\#(15,15) = 68$	68		68				68		68	
	$\#(5,1) = 2$	2		1				1		0	
	$\#(3,3) = 1$	1		1				0		0	
	$\#(5,-3) = 1$	0		1				0		1	
$n = 21, p = 3$	$\#(1,1) = 1$	-	-	1	-	-	-	0	-	-	Do
$\lambda = 2048$	$\#(21,-7) = 37449$			18688				18761			not
$(21, 7, -, -)$	$\#(21,21) = 12480$			6251				6227			exist
	$\#(7,7) = 9$			8				7			
	$\#(3,-1) = 1$			0				1			

3 Investigation of the ${}_n\mathcal{H}$ Matrix

Investigation of the ${}_n\mathcal{H}$ matrix construction is at least important in sense of improving search strategies for functions on larger number of variables. In this section we investigate the structure of the matrix ${}_n\mathcal{H}$ when n is prime and appropriately chosen.

Let $x = (x_0, x_1, \ldots, x_{l-1})^T$ be some vector. We introduce the permutation matrix π_l of size $l \times l$ such that $\pi_l \cdot x = (x_{l-1}, x_0, \ldots, x_{l-2})$, i.e., the matrix π_l generates a cyclic shift by 1 position on an alphabet of l symbols. Note also that $(\pi_l \cdot x)^T = x^T \cdot \pi_l^T = x^T \cdot \pi_l^{-1}$. By $[\pi_l^{ai+b} \cdot x]$ we denote the matrix of size $l \times l$ of the form

$$[\pi_l^{ai+b} \cdot x] = [\pi_l^{a\cdot 0+b} x \quad \pi_l^{a\cdot 1+b} x \quad \ldots \quad \pi_l^{a\cdot(l-1)+b} x] = \begin{pmatrix} x_b & x_{a+b} & \cdots & x_{a(l-1)+b} \\ x_{b+1} & x_{a+b+1} & & x_{a(l-1)+b+1} \\ \vdots & & \ddots & \vdots \\ x_{b+l-1} & x_{a+b+l-1} & \cdots & x_{a(l-1)+b+l-1} \end{pmatrix}, \quad (7)$$

where all indices are taken modulo l. Let us introduce a new symbol

$$\begin{bmatrix} \mathsf{b} \\ t_i \end{bmatrix} = [\pi_l^{1i+b} \cdot t_i],$$

where t_i is some vector of size l. Thus, the square matrix $\begin{bmatrix} \mathsf{b} \\ t_i \end{bmatrix}$ is such that each column is the cyclic shift by 1 of the previous column.

Lemma 3. *For n prime $\left(2^{\frac{n-1}{2}} - 1\right) \mid \left(\frac{g_n}{2} - 1\right)$ iff the Legendre symbol $(2/n)$ is -1.*

Proof:

For prime n $d_{n,1} = 2$, $d_{n,n} = \frac{1}{n}\mu(\frac{n}{1})2^1 + \frac{1}{n}\mu(\frac{n}{n})2^n = \frac{2^n-2}{n}$, and all the rest $d_{n,t}$ are 0. Hence, $\frac{g_n}{2} - 1 = \frac{1}{2}(d_{n,1} + d_{n,n}) - 1 = \frac{2^{n-1}-1}{n} = \frac{(2^{(n-1)/2}-1)(2^{(n-1)/2}+1)}{n}$. The denominator n divides one of the multiples in the product. Therefore, we get that $\left(2^{\frac{n-1}{2}} - 1\right) \mid \frac{g_n}{2} - 1$ only if $2^{(n-1)/2} + 1 \equiv 0 \mod n$, i.e., $(2/n) \equiv -1 \mod n$. □

Denote the matrix ${}^*_n\mathcal{H}$ to be the matrix ${}_n\mathcal{H}$ for which one row and one column, both represented by $\Lambda_0 = (00\ldots0)$, are removed. The size of ${}^*_n\mathcal{H}$ is $(\frac{g_n}{2} - 1) \times (\frac{g_n}{2} - 1)$. Futher results are based on the following observation.

Observation 1 *For n odd prime when $(2/p) = -1$, the representative elements for rows and columns of ${}^*_n\mathcal{H}$ can be permuted by Algorithm$^\pi$ such that it is constructed by sub matrices of size $(l \times l) = (2^{\frac{n-1}{2}} - 1) \times (2^{\frac{n-1}{2}} - 1)$ (see Lemma 3), each of the form $\begin{bmatrix} \mathsf{b} \\ t_i \end{bmatrix}$, where t_i's are some fixed vectors of size l.*

For abuse of notation we define:

$$\begin{aligned} \mathsf{sz} &\text{– the size of sub matrices } \begin{bmatrix} \mathsf{b} \\ t_i \end{bmatrix} \text{ of the matrix } {}^*_n\mathcal{H}; \\ m_{\mathsf{num}} &\text{– the number of sub matrices in } {}^*_n\mathcal{H}; \\ v_{\mathsf{num}} &\text{– the number of different vectors used to represent } {}^*_n\mathcal{H} \text{ in the } \begin{bmatrix} \mathsf{b} \\ t_i \end{bmatrix} \text{ form.} \end{aligned} \tag{8}$$

Algorithm$^\pi$: Permutation of ${}_n\mathcal{H}$ for Observation 1

input: n — odd prime such that $(2/n) = -1$, denotes the number of variables
${}^*_n\mathcal{H}[i][j]$ — reduced ${}_n\mathcal{H}$ matrix, $i, j = [0, \ldots, \frac{g_n}{2} - 1]$
output: permuted ${}^*_n\mathcal{H}$

(1) Constants: $\mathsf{sz} = 2^{\frac{n-1}{2}} - 1$; $m_{\mathsf{num}} = \frac{1}{n}(2^{\frac{n-1}{2}} + 1)$; $p_0 = -n + 2$ - the values to be placed on the main diagonal of ${}^*_n\mathcal{H}$; $p_1 = n - 4$ - the values to be placed along the main diagonal;
(2) *First permutation*
for $d = 0 \ldots m_{\mathsf{num}} - 1$
| in the row $d * \mathsf{sz}$ find p_0 at some position $i \geq d * \mathsf{sz}$. Swap columns $(i, d * m_{\mathsf{num}})$;
| in the column $d * \mathsf{sz}$ find p_1 at some position $i > d * \mathsf{sz}$. Swap rows $(i, d * m_{\mathsf{num}} + 1)$;
| in the row $d * \mathsf{sz} + 1$ find p_0 at some position $i > d * \mathsf{sz}$. Swap columns $(i, d * m_{\mathsf{num}} + 1)$;
| for $k = 1 \ldots \mathsf{sz} - 2$
| | find $i > d * \mathsf{sz} + k$ such that ${}^*_n\mathcal{H}[i][d * \mathsf{sz} + k - 1] = {}^*_n\mathcal{H}[i][d * \mathsf{sz} + k] = p_1$.
| | Swap the rows $(i, d * \mathsf{sz} + k + 1)$;
| | find $i > d * \mathsf{sz} + k$ such that ${}^*_n\mathcal{H}[d * \mathsf{sz} + k + 1][i] = p_0$.
| | Swap the columns $(i, d * \mathsf{sz} + k + 1)$;
(3) *Refining permutation*
Now the matrix ${}^*_n\mathcal{H}$ consists of sub matrices of the form $[\pi^{a \cdot i + b}_{\mathsf{sz}} \cdot t_x]$.
We continue to refine the structure of ${}^*_n\mathcal{H}$ by the following steps:
a) for each $d = 1 \ldots m_{\mathsf{num}} - 1$ consider the sub matrix ${}^*_n\mathcal{H}[0 \ldots \mathsf{sz} - 1][d * \mathsf{sz} \ldots (d + 1) * \mathsf{sz} - 1]$, which is of the form $[\pi^{a \cdot i + b}_{\mathsf{sz}} \cdot t_x]$. Since $\gcd(a, \mathsf{sz}) = 1$, it is possible to permute the rows in the matrix ${}^*_n\mathcal{H}$ s.t. the form of the sub matrix becomes to be $[\pi^{1 \cdot i + b}_{\mathsf{sz}} \cdot t_x]$, i.e., $\begin{bmatrix} \mathsf{b}' \\ t_x \end{bmatrix}$. If we enumerate the rows of the sub matrix as $\{0, 1, 2, \ldots, \mathsf{sz} - 1\}$, then the desired permutation is $\{0a, 1a, 2a, \ldots, (\mathsf{sz} - 1)a\} \mod (\mathsf{sz})$ give us the sub matrix $\begin{bmatrix} \mathsf{b}' \\ t_x \end{bmatrix}$;
b) for each $d = 1 \ldots m_{\mathsf{num}} - 1$ consider the sub matrix ${}^*_n\mathcal{H}[d * \mathsf{sz} \ldots (d + 1) * \mathsf{sz} - 1][0 \ldots \mathsf{sz} - 1]$, which again can be of the form $[\pi^{a \cdot i + b}_{\mathsf{sz}} \cdot t_x]$. We can transform this sub matrix to the form $\begin{bmatrix} \mathsf{b}' \\ t_y \end{bmatrix}$ permuting the corresponding columns of ${}^*_n\mathcal{H}$ in a similar way as in (a).

The result of Algorithm$^\pi$ is that all sub matrices of ${}^*_n\mathcal{H}$ become to be of the form $\begin{bmatrix} \mathsf{b} \\ t_x \end{bmatrix}$, where b and t_x can be different for each sub matrix. However, the observation above is not proved yet, it is an open question. The first primes for which such permutation can be applied are $n = 3, 5, 11, 13, 19, 29, 37, 43, \ldots$, according to Lemma 3. For example, permuted ${}_5\mathcal{H}$ (with Λ_0-row and column) for $n = 5$ looks like this (see also (1)):

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 5 & -3 & 1 & 1 \\ 5 & 1 & -3 & 1 \\ 5 & 1 & 1 & -3 \end{pmatrix}, \tag{9}$$

where the representative elements for the rows are in the order: $(00000), (00011), (00101), (01111)$; and for the columns are in the order: $(00000), (00101), (00011), (01111)$. There is only 1 sub matrix, which is denoted as $\begin{bmatrix} \mathsf{0} \\ t_0 \end{bmatrix}$, where $t_0 = \{-3, 1, 1\}^T$.

For notation purposes let us introduce a new matrix ${}_n\mathcal{M}$ to be the matrix of size $m_{\mathsf{num}} \times m_{\mathsf{num}}$, where each cell contains the corresponding sub matrix of ${}^*_n\mathcal{H}$, after Algorithm$^\pi$, i.e., ${}^*_n\mathcal{H} = {}_n\mathcal{M}$,

which means that ${}^{*}_{n}\mathcal{H}$ can be written now in a short way via the matrix ${}_n\mathcal{M}$, since each cell is a sub matrix of the form $\begin{bmatrix} \mathsf{b} \\ t_x \end{bmatrix}$. In the example above with $n = 5$ the matrix ${}_n\mathcal{M}$ is of size 1×1, and ${}_n\mathcal{M}[0][0] = \begin{bmatrix} \mathsf{0} \\ t_0 \end{bmatrix}$.

As a bit larger example we present the structure of the ${}_n\mathcal{H}$-matrix for $n = 11$ variables: ${}_{11}\mathcal{M}$ is of size 3×3 and $g_{11} = 188$; the number of different vectors is 2, their size is 31:
$t_0 =$ { -9, 7, 7, 3, 7, 3, 3, -5, 7, 3, 3, -1, 3, -1, -5, -1, 7, 3, 3, -5, 3, -1, -1, -1, 3, -5, -1, -1, -5, -1, -1 }^{T}
$t_1 =$ { 3, 3, 3, -1, -1, -1, -5, 3, -1, -1, 3, -1, -1, -1, -1, -1, -5, -1, 3, -5, 3, -1, 3, 3, -1, -5, -1, 3, -1, -1, -5 }^{T}

$$ {}_{11}\mathcal{M} = \begin{pmatrix} \begin{bmatrix} \mathsf{0} \\ t_0 \end{bmatrix} & \begin{bmatrix} \mathsf{0} \\ t_1 \end{bmatrix} & \begin{bmatrix} \mathsf{0} \\ t_1 \end{bmatrix} \\ \begin{bmatrix} \mathsf{0} \\ t_1 \end{bmatrix} & \begin{bmatrix} \mathsf{26} \\ t_0 \end{bmatrix} & \begin{bmatrix} \mathsf{13} \\ t_1 \end{bmatrix} \\ \begin{bmatrix} \mathsf{0} \\ t_1 \end{bmatrix} & \begin{bmatrix} \mathsf{13} \\ t_1 \end{bmatrix} & \begin{bmatrix} \mathsf{26} \\ t_0 \end{bmatrix} \end{pmatrix} \tag{10} $$

For the complete and detailed description of ${}_{11}\mathcal{H}$ and ${}_{13}\mathcal{H}$, including the order of representative elements for ${}_n\mathcal{H}$, one can see Appendix B1 and Appendix B2, respectively. The structure of ${}_{19}\mathcal{M}$ is presented in Appendix B3, in order to see clearly that the second observation (see further) works.

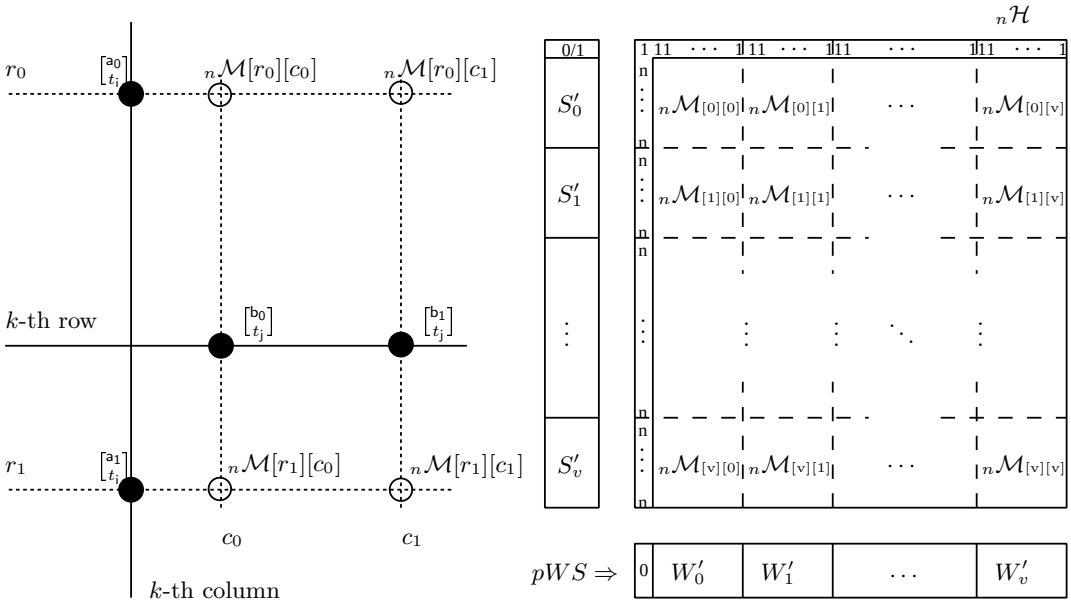

Fig. 1. Property of ${}_n\mathcal{M}$ (left), and data structures for ${}_n\mathcal{H}$ after Algorithm$^{\pi}$ (right).

In Figure 1 (right) the structure of permuted matrix ${}_n\mathcal{H}$ in terms of the matrix ${}_n\mathcal{M}$ is depicted. Now we make the second observation, in particular, the property of the matrix ${}_n\mathcal{M}$.

Observation 2 *If n is odd prime for which $(2/n) = -1$, then the matrix ${}_n\mathcal{M}$ has the following properties:*

(i) the main diagonal is represented by the same vector t_0, i.e., ${}_n\mathcal{M}[k][k] = \begin{bmatrix} \mathsf{b}_k \\ t_0 \end{bmatrix}$;
(ii) each row (column) contains exactly one item with t_0, whereas all the rest items with vectors t_i are doubled in the same row (column);
(iii) the matrix is symmetric, i.e., ${}_n\mathcal{M}[i][j] = {}_n\mathcal{M}[j][i]$;
(iv) select k-th row and k-th column (as shown in Figure 1 (left)). For $i, j = 1, \ldots, \frac{n-1}{2}$ there are exactly two rows r_0 and r_1 (according to (ii)), for which ${}_n\mathcal{M}[r_0][k] = \begin{bmatrix} \mathsf{a}_0 \\ t_i \end{bmatrix}$ and ${}_n\mathcal{M}[r_1][k] = \begin{bmatrix} \mathsf{a}_1 \\ t_i \end{bmatrix}$ (the same t_i), and there are exactly two columns c_0 and c_1 where ${}_n\mathcal{M}[k][c_0] = \begin{bmatrix} \mathsf{b}_0 \\ t_j \end{bmatrix}$ and

${}_n\mathcal{M}[k][c_1] = \left[\begin{smallmatrix}\mathsf{b}_1\\ t_j\end{smallmatrix}\right]$. *The following property holds:*

$$\begin{cases} {}_n\mathcal{M}[r_0][c_0] &= \pi^{a_0-a_1+b_0-b_1}\,{}_n\mathcal{M}[r_1][c_1] \\ {}_n\mathcal{M}[r_0][c_1] &= \pi^{a_0-a_1-b_0+b_1}\,{}_n\mathcal{M}[r_1][c_0]. \end{cases} \tag{11}$$

□

4 Transformation Technique on Walsh Spectra: Method to Construct a Group of New Plateaued RSBFs

Assume we have found one balanced plateaued RSBF on n odd prime number of variables when $(2/n) = -1$. We will show how the results from the previous section can be used to create many balanced plateaued functions from the known one. Moreover, we will show that the Walsh spectra for these new functions will be a permutation of the Walsh spectra of the initial function, and we also derive the transformation rules to generate these new functions.

Assume we have one balanced PRSBF, then its the first half-RSTT can be written as $(S'_0, \ldots, S'_{m_{\mathsf{num}}-1})$ – a set of row-vectors (we do not consider the value for Λ_0), and the second half-RSTT is $(S''_0, \ldots, S''_{m_{\mathsf{num}}-1})$, as shown in Figure 1 (right). The first partial Walsh Spectra (without the point corresponding the column Λ_0) is $(W'_0, \ldots, W'_{m_{\mathsf{num}}-1})$ – a set of row-vectors, where

$$W'_k = \sum_{i=0}^{m_{\mathsf{num}}-1} S'_i \cdot {}_n\mathcal{M}[i][k],$$

and similar for the second $pWS = (W''_0, \ldots, W''_{m_{\mathsf{num}}-1})$. The sub part of RSTT S'_i corresponds to the representative elements in the vector $R_{r,i}$. The sub part of pWS W'_j corresponds to the representative elements in the vector $R_{c,j}$. Schematicaly, the data structures are shown in Figure 1 (right). Note, that if any two rows ($\neq \Lambda_0$) are swapped, then the function is still balanced, since all rows, except Λ_0, at the column Λ_0 have the same value, equal to n.

Theorem 2. *Let n is odd prime for which $(2/n) = -1$. The following basic transformations of the first half-RSTT $(S'_0, \ldots, S'_{m_{\mathsf{num}}-1})$ permute the partial Walsh spectra $(W'_0, \ldots, W'_{m_{\mathsf{num}}-1})$, but remain Walsh transform for the column Λ_0 unchanged:*

T1. *The "local" cyclic shift $S'_i \to S'_i \cdot \pi^a$ in each sub-RSTT for all $i = 0, \ldots, m_{\mathsf{num}} - 1$ results in a locally cyclic shifted pWS as: $W'_i \to W'_i \cdot \pi^{-a}$, for all i;*

T2. *Based on Observation 2(iv) we can perform swaps of S'_i's. For any parameter of this kind of transformation $k = 0, \ldots, v_{\mathsf{num}} - 1$ the basic operation is:*
For all different pairs (r_0, r_1) for which ${}_n\mathcal{M}[r_0][k] = \left[\begin{smallmatrix}\mathsf{a}_0\\ t_x\end{smallmatrix}\right]$ and ${}_n\mathcal{M}[r_1][k] = \left[\begin{smallmatrix}\mathsf{a}_1\\ t_x\end{smallmatrix}\right]$ substitute the sub-RSTTs as $(S'_{r_0}, S'_{r_1}) \to (S'_{r_1} \cdot \pi^{a_1-a_0}, S'_{r_0} \cdot \pi^{a_0-a_1})$, i.e., swap and cyclic shift. This will permute the pWS in the similar way, i.e., for all pairs (c_0, c_1), for which ${}_n\mathcal{M}[k][c_0] = \left[\begin{smallmatrix}\mathsf{b}_0\\ t_y\end{smallmatrix}\right]$ and ${}_n\mathcal{M}[k][c_1] = \left[\begin{smallmatrix}\mathsf{b}_1\\ t_y\end{smallmatrix}\right]$ the transformation becomes $(W'_{c_0}, W'_{c_1}) \to (W'_{c_1} \cdot \pi^{b_1-b_0}, W'_{c_0} \cdot \pi^{b_0-b_1})$.

Proof:

1) A new pWS after such permutation is equal to

$$\sum_{l=0}^{m_{\mathsf{num}}-1} S'_l \cdot \pi^a \cdot {}_n\mathcal{M}[l][i] = \sum_{i=0}^{m_{\mathsf{num}}-1} S'_l \cdot {}_n\mathcal{M}[l][i] \cdot \pi^{-a} = W'_i \cdot \pi^{-a};$$

2) Consider the values r_0, r_1, c_0, c_1, such that ${}_n\mathcal{M}[r_0][k] = \left[\begin{smallmatrix}\mathsf{a}_0\\ t_x\end{smallmatrix}\right]$, ${}_n\mathcal{M}[r_1][k] = \left[\begin{smallmatrix}\mathsf{a}_1\\ t_x\end{smallmatrix}\right]$, ${}_n\mathcal{M}[k][c_0] = \left[\begin{smallmatrix}\mathsf{b}_0\\ t_y\end{smallmatrix}\right]$, ${}_n\mathcal{M}[k][c_1] = \left[\begin{smallmatrix}\mathsf{b}_1\\ t_y\end{smallmatrix}\right]$. Let l_0 and l_1 denote the sum contributed by the sub-RSTTs S'_{r_0} and S'_{r_1} in W'_{c_0} and W'_{c_1}, respectively, before the transformation. Then

$$\begin{cases} l_0 &= S'_{r_0} \cdot {}_n\mathcal{M}[r_0][c_0] + S'_{r_1} \cdot {}_n\mathcal{M}[r_1][c_0] \\ l_1 &= S'_{r_0} \cdot {}_n\mathcal{M}[r_0][c_1] + S'_{r_1} \cdot {}_n\mathcal{M}[r_1][c_1]. \end{cases}$$

After the substitution $(S'_{r_0}, S'_{r_1}) \to (S'_{r_1} \cdot \pi^{a_1-a_0}, S'_{r_0} \cdot \pi^{a_0-a_1})$ for the same columns c_0 and c_1 the contribution will be changed $l_0 \to l'_0$ and $l_1 \to l'_1$ as follows:

$$\begin{cases} l'_0 &= S'_{r_1} \cdot \pi^{a_1-a_0} \cdot {}_n\mathcal{M}[r_0][c_0] + S'_{r_0} \cdot \pi^{a_0-a_1} \cdot {}_n\mathcal{M}[r_1][c_0] \\ l'_1 &= S'_{r_1} \cdot \pi^{a_1-a_0} \cdot {}_n\mathcal{M}[r_0][c_1] + S'_{r_0} \cdot \pi^{a_0-a_1} \cdot {}_n\mathcal{M}[r_1][c_1]. \end{cases}$$

With Observation 2(iv) we rewrite:

$$\begin{cases} l'_0 &= S'_{r_1} \cdot \pi^{a_1-a_0} \cdot \pi^{a_0-a_1+b_0-b_1} \cdot {}_n\mathcal{M}[r_1][c_1] + S'_{r_0} \cdot \pi^{a_0-a_1} \cdot \pi^{a_1-a_0+b_0-b_1} \cdot {}_n\mathcal{M}[r_0][c_1] \\ l'_1 &= S'_{r_1} \cdot \pi^{a_1-a_0} \cdot \pi^{a_0-a_1+b_1-b_0} \cdot {}_n\mathcal{M}[r_1][c_0] + S'_{r_0} \cdot \pi^{a_0-a_1} \cdot \pi^{a_1-a_0+b_1-b_0} \cdot {}_n\mathcal{M}[r_0][c_0] \end{cases}$$

$$\Rightarrow \begin{cases} l'_0 &= S'_{r_1} {}_n\mathcal{M}[r_1][c_1]\pi^{b_1-b_0} + S'_{r_0} {}_n\mathcal{M}[r_0][c_1]\pi^{b_1-b_0} \\ l'_1 &= S'_{r_1} {}_n\mathcal{M}[r_1][c_0]\pi^{b_0-b_1} + S'_{r_0} {}_n\mathcal{M}[r_0][c_0]\pi^{b_0-b_1} \end{cases} \Rightarrow \begin{cases} l'_0 &= l_1\pi^{b_1-b_0} \\ l'_1 &= l_0\pi^{b_0-b_1} \end{cases}$$

Since b's do not depend on rows, then after the transformation $(S'_{r_0}, S'_{r_1}) \to (S'_{r_1} \cdot \pi^{a_1-a_0}, S'_{r_0} \cdot \pi^{a_0-a_1})$ for all $i = 0, \ldots, v_{\mathsf{num}} - 1$, the partial Walsh spectra will be transformed accordingly as $(W'_{c_0}, W'_{c_1}) \to (W'_{c_1} \cdot \pi^{b_1-b_0}, W'_{c_0} \cdot \pi^{b_0-b_1})$, for all $i = 1, \ldots, v_{\mathsf{num}} - 1$.

□

If the transformation operations **T1** and **T2** are done in parallel for both S'_*'s and S''_*'s, then, obviously, they result in a new balanced/unbalanced PRSBF. The number of different mixtured transformations that generate a new PRSBF is given as follows.

Corollary 2. *The number of joint transformations is*

$$\left(\frac{2^{\frac{n-1}{2}}+1}{n}\right)! \cdot \left(2^{\frac{n-1}{2}}-1\right) \quad . \tag{12}$$

Proof:

Note, that $n | \left(2^{\frac{n-1}{2}}+1\right)$, otherwise $(2/n) \neq -1$. The number of permutations of the form **T1** is the size of sub matrices sz. We can also note that since the main diagonal of ${}_n\mathcal{M}$ is filled with t_0-items, all the permutations of the second kind **T2** are "orthogonal", and any possible permutation of S'_i's can be then achieved by a sequence of transformations of the second kind.

□

The result above means that in searching for PRSBFs we do not need to worry much about highest resiliency property, because it can be derived by manipulations on Walsh spectra (means that the corresponding manipulations must be done on RSTT). We have implemented this manipulation technique on a usual PC, and tested on different instances.

As an example, after several days of searching for a PRSBF in our simulations we have found (by luck) a 0-resilient PRSBF on $n = 11$ number of variables with amplitude $\lambda = 64$. Using the manipulation tecnique we could construct 185 *new* PRSBFs, and the best was a 2-resilient $(11, 2, -, -)$ plateaued RSBF with $\lambda = 64$. Here is the truth table (2^{11} points) of this function in hexadecimal representation (first bit is for the input $(00\ldots0)$, etc.):

```
7ACCA5B1 8D769E57 84B63A39 92AC273A 80348F3D 4FDC5EC2 9359C8E0 193B0BD9
C5000F71 91BE0AE6 64BBF2F5 76E9F119 961A2793 E094F901 47C34E8F 15DBF283
B4775014 15FE2A02 C613CBE8 4498ED68 7970CACE AB1CFF32 6F6DFCC6 AA4602D3
977956CD 1C7BD60E FC44C721 EE831552 616BE15A 25B885FA 0333A2DA EF0C904F
CA353E6F 26454234 0637BEE8 5D88551D B03D560A A5CFE9D5 643586D1 B9A37DC1
6FC67E00 A598A4B8 DC8A16F4 BBEA0A0D 7DEB6DE2 EAB1A17C 999C343C 150CB24B
876B2B86 2768F0F7 47E03B9F A72D51F9 BAE03424 E06E5803 F9B8851E 56667249
391238CF B85733DD 48628AC1 D436EAC9 544B4F5F 8809E689 E9BF01A1 971175FF
```

References

1. P. Stănică, S. Maitra and J. Clark. Results on rotation symmetric bent and correlation immune boolean functions. In *Fast Software Encryption 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 161–177. Springer-Verlag, 2004.
2. P. Sarkar and S. Maitra. Construction of nonlinear boolean functions with important cryptographic properties. In *Advances in Cryptology—EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 485–506. Springer-Verlag, 2000.
3. P. Sarkar and S. Maitra. Nonlinearity bounds and construction of resilient boolean functions. In *Advances in Cryptology—CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 515–532. Springer-Verlag, 2000.
4. E. Pasalic W. Meier and C. Carlet. Algebraic attacks and decomposition of boolean functions. In *Advances in Cryptology—EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 474–491. Springer-Verlag, 2004.
5. E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology—EUROCRYPT'98*, Lecture Notes in Computer Science. Springer-Verlag, 1998.
6. Josef Pieprzyk and Cheng Xin Qu. Rotation-symmetric functions and fast hashing. In *Proceedings of the Third Australasian Conference on Information Security and Privacy*, pages 169–180. Springer-Verlag, 1998.
7. P. Stănică and S. Maitra. Rotation symmetric boolean functions – count and cryptographic properties. In R. C. Bose Centenary Symposium on Discrete Mathematics and Applications, volume 15 of *Electronic Notes in Discrete Mathematics*. Elsevier, 2002.
8. T. W. Cusick, P. Stănică. Fast evaluation, weights and nonlinearity of rotation-symmetric functions. *Discrete Math.*, 258 (1–3):289–301, 2002.
9. J. Clark, J. Jacob, S. Maitra and P. Stănică. Almost boolean functions: The design of boolean functions by spectral inversion. In *The 2003 Congress on Evolutionary Computation*, volume 3, pages 2173–2180. IEEE Transactions on Information Theory, 2003.
10. K. C. Gupta D. K. Dalai and S. Maitra. Results on algebraic immunity for cryptographically significant boolean functions. In *submitted to INDIACRYPT 2004*, 2004.
11. A. Maximov M. Hell and S. Maitra. On efficient implementation of search strategy for rotation symmetric boolean functions. In *9th International Workshop on Algebraic and Combinatorial Coding Theory — ACCT 2004, June 19-25, 2004, Black Sea Coast, Bulgaria*, 2004.
12. M. Hell A. Maximov and S. Maitra. Plateaued rotation symmetric boolean functions on odd number of variables. Available at IACR eprint server, eprint.iacr.org, no. 2004/144, 25 June 2004, 2004.
13. GSM Association. Technical specification: 3GPP TS 55.218 v6.1.0 (2002-12), 2002. *http://www.3gpp.org/*.
14. D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi, and B. Preneel. A new keystream generator MUGI. In J. Daemen and V. Rijmen, editors, *Fast Software Encryption 2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 179–194. Springer-Verlag, 2002.
15. K. Nyberg. Generalized feistel networks. In *Advances in Cryptology—ASIACRYPT'96*, volume 1163 of *Lecture Notes in Computer Science*, pages 91–104. Springer-Verlag, 1996.
16. H. Feistel. Cryptography and computer privacy, May 1973.
17. Y. Zheng and X. M. Zhang. Plateaued functions. In *ICICS—1999*, volume 1726 of *Lecture Notes in Computer Science*, pages 284–300. Springer-Verlag, 1999.
18. C. Carlet and E. Prouff. On plateaued functions and their constructions. In *Fast Software Encryption 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 54–73. Springer-Verlag, 2003.
19. unknown author. On rotation symmetric boolean functions of even number of variables, 2004.
20. William J. LeVeque. *Fundamentals of Number Theory*. Dover Publications, Inc., 1977.

Appendix A: Proofs

A1. Proof for Lemma 2

(i) Let for some row i the representative element is Λ, then the value ${}_n\mathcal{H}_{i,\Lambda_0} = \sum_{x\in G(\Lambda)}(-1)^{x\cdot 0}$, and is actually equal to the number of summands, i.e., the number of elements in the group $G(\Lambda)$.

(ii) Let the group at i-th row corresponds to some representative element $\Lambda = (a_{n-1}a_{n-2}\dots a_0)$, and let $I_0 = \{0, p, 2p, \dots, (\frac{n}{p}-1)p\}$ be the set of indices taken modulo t, and its size is n/p. Define p sums:

$$c_i = \sum_{j\in(i+I_0)} a_j \pmod t, \quad \text{where } i = 0, 1, \dots, p-1. \tag{13}$$

Define also $h = \sum_{i=0}^{p-1} c_i$ — the number of $c_i = 1$. Then, obviously, ${}_n\mathcal{H}_{\Lambda,\Lambda_p} = ((-1)\cdot h + (+1)\cdot (p-h))\frac{n}{p}\cdot\frac{t}{n} = (t - \frac{2t}{p}h)$. The value ${}_n\mathcal{H}_{\Lambda,\Lambda_p}$ now depends only on the value $h \in [0\dots p-1]$. Consider $l = \mathrm{lcm}(p,t)$ then $\{0, p, 2p, \dots, (l-1)p\} \equiv \{l\cdot p, (l+1)p, (l+2)p, \dots, (2l-1)p\} \mod t$. Then $a_{i \mod t} = a_{(i+l) \mod t}$, and, hence, we can now redefine the set of indices I_0 such that the values c_i's are unchanged: $I_0 = \{0, p, 2p, \dots, (l/p-1)p\}$, which is of size l now. Also note that since p is prime, $l = \mathrm{lcm}(p,t)$ can only be t or $p\cdot t$.

Let $p_t(h)$ is the number of values $x \in \{0,1\}^n$ such that $\rho_n^t(x) = x$ and for these x the number of $c_i : c_i = 0$ is h. To calculate the value p_t consider two cases:

(a) if $\gcd(p,t) = p$, then $p|t$. Then consider $I_0 = \{0, p, 2p, \dots, (l-1)p\} \mod t$ has t/p values, and for any $i = 0, \dots, p-1 \Rightarrow (a + I_0)\cap I_0 \equiv \emptyset$. It means that the values for $t-p$ points of x can be chosen randomly, and the rest values for p point correspond to the certain values of c_i's. In this case $p_t = \binom{p}{h}\cdot 2^{t-p}$;

(b) if $\gcd(p,t) = 1$, then $\mathrm{lcm}(p,t) = p\cdot t$, and $I_0 = \{0, p, 2p, \dots, (\frac{p\cdot t}{p}-1)p\} \equiv \{0, 1, 2, \dots, (t-1)p\} \mod t$, i.e., for any $i = 0, \dots, p-1 \Rightarrow (i + I_0) \equiv I_0 \mod t$. It means that $c_0 = c_1 = \dots = c_{p-1}$. The representative element Λ is even, and its weight is $h\cdot\frac{n}{p}$ and must be even. Hence, all c_i's are 0, i.e., $p_t = 1$ if $h = 0$, otherwise $p_t = 0$. Note, by the similar reasons h is even, i.e. $h = 2r$ for some $r = [0\dots\frac{n-1}{2}]$.

Combining a) and b) we found $p_t = \binom{p}{h}\cdot q_t$, where q_t is defined as in (5). Let $d_t(h)$ be the number of groups where the elements such that $\rho_n^t(x) = x$, and h number of c_i's are 1's. Note also that h is the same for all elements of the same group. The recursive function for $d_t(h)$ is:

$$d_t(h) = \frac{1}{t}(p_t(h) - \sum_{k|t, k<t} k\cdot d_k(h)) \Rightarrow p_t(h) = \sum_{k|t} k\cdot d_k(h)$$

We use the Möbius function to invert the expression:

$$d_t(h) = \frac{1}{t}\sum_{k|t}\mu(t/k)p_k,$$

from which the result follows.

□

A2. Proof for Theorem 1

Assume there is a Boolean function $\sigma = (\sigma_1||\sigma_2)$, for which the partial Walsh spectras for the column Λ_0 are $\tau_1\lambda/2$ and $-\tau_1\lambda/2$, and for the column Λ_p are both $\tau_2\lambda/2$. We represent the column Λ_0 as a set of m blocks, each containing p_i numbers of a_i. The first half of the function can be characterized by the set $k'_0\dots k'_{m-1}$ — the number of 0's in each block. Obviously, k'_i is bounded by $[0\dots p_i]$. The same we can say for the second half of the Boolean function. Assume we found k_i^*'s, then partial Walsh spectras are expressed

1) For the column Λ_0: $pWS_{\Lambda_0} = \sum_{i=0}^{m-1}(a_i \cdot k_i^* - a_i(p_i - k_i^*)) = -\tau_1\lambda/2$ or $+\tau_1\lambda/2 \Rightarrow \sum_{i=0}^{m-1}(2a_i \cdot k_i^*) - \sum_{i=0}^{m-1}(a_i \cdot p_i) = \pm\tau_1\lambda/2 \Rightarrow \sum_{i=0}^{m-1} a_i k_i' = \frac{\tau_1\lambda+2^n}{4}$ and $\sum_{i=0}^{m-1} a_i k_i'' = \frac{-\tau_1\lambda+2^n}{4}$.
2) For the column Λ_p by the same way we get a similar formula (instead of a_i's we use b_i's, and instead of $(+\tau_1, -\tau_1)$ solution we should test for $(+\tau_2, +\tau_2)$ solution). □

Appendix B1: The structure of ${}_{11}\mathcal{H}$

${}_{11}\mathcal{M}$ is of size 3×3, $g_{11} = 188$. The number of different vectors is 2, their size is 31:
$t_0 =$ { -9, 7, 7, 3, 7, 3, 3, -5, 7, 3, 3, -1, 3, -1, -5, -1, 7, 3, 3, -5, 3, -1, -1, -1, 3, -5, -1, -1, -5, -1, -1 }^{T}
$t_1 =$ { 3, 3, 3, -1, -1, -1, -5, 3, -1, -1, 3, -1, -1, -1, -1, -1, -5, -1, 3, -5, 3, -1, 3, 3, -1, -5, -1, 3, -1, -1, -5 }^{T}

$$ {}_{11}\mathcal{M} = \begin{pmatrix} \begin{bmatrix}0\\t_0\end{bmatrix} & \begin{bmatrix}0\\t_1\end{bmatrix} & \begin{bmatrix}0\\t_1\end{bmatrix} \\ \begin{bmatrix}0\\t_1\end{bmatrix} & \begin{bmatrix}26\\t_0\end{bmatrix} & \begin{bmatrix}13\\t_1\end{bmatrix} \\ \begin{bmatrix}0\\t_1\end{bmatrix} & \begin{bmatrix}13\\t_1\end{bmatrix} & \begin{bmatrix}26\\t_0\end{bmatrix} \end{pmatrix} \tag{14} $$

Representative elements for rows of ${}_{11}\mathcal{H}$ are in the order: 0, 3, 5, 15, 17, 51, 85, 255, 9, 27, 45, 119, 153, 427, 703, 63, 33, 99, 165, 495, 163, 335, 189, 231, 293, 879, 219, 365, 887, 411, 683, 1023, 39, 105, 187, 423, 349, 479, 83, 245, 249, 89, 235, 317, 237, 311, 363, 751, 243, 169, 507, 53, 95, 71, 201, 347, 763, 111, 139, 413, 469, 509, 29, 57, 75, 221, 359, 373, 503, 101, 175, 159, 77, 215, 303, 183, 315, 429, 759, 207, 149, 447, 43, 125, 113, 147, 437, 735, 123, 141, 371, 343, 383, 23.

Representative elements for columns of ${}_{11}\mathcal{H}$ are in the order: 0, 683, 411, 887, 365, 219, 879, 293, 231, 189, 335, 163, 495, 165, 99, 33, 63, 703, 427, 153, 119, 45, 27, 9, 255, 85, 51, 17, 15, 5, 3, 1023, 509, 469, 413, 139, 111, 763, 347, 201, 71, 95, 53, 507, 169, 243, 751, 363, 311, 237, 317, 235, 89, 249, 245, 83, 479, 349, 423, 187, 105, 39, 29, 383, 343, 371, 141, 123, 735, 437, 147, 113, 125, 43, 447, 149, 207, 759, 429, 315, 183, 303, 215, 77, 159, 175, 101, 503, 373, 359, 221, 75, 57, 23.

Appendix B2: The structure of ${}_{13}\mathcal{H}$

${}_{13}\mathcal{M}$ is of size 5×5, $g_{13} = 632$. The number of different vectors is 3, their size is 63:
$t_0 =$ { -11, 9, 9, 5, 9, 5, 5, -3, 9, 5, 5, -3, 5, 1, -3, -7, 9, 5, 5, 1, 5, 1, -3, 1, 5, -3, 1, -3, -3, 1, -7, 1, 9, 5, 5, -3, 5, -3, 1, -7, 5, 1, 1, 1, -3, -3, 1, 1, 5, -3, -3, -7, 1, 1, -3, 1, -3, -7, 1, 1, -7, 1, 1 }^{T}
$t_1 =$ { -3, 1, 1, 1, -3, -7, 5, 1, 1, 1, 1, -7, 1, 5, 1, 1, -3, 1, -3, 5, -3, 1, -3, -3, -3, -3, 1, 5, 1, 1, -3, -3, 1, -3, -7, 5, 1, 5, 5, 1, -3, -3, 1, 1, -7, 1, 5, -3, 5, -3, 5, 1, 1, -3, 1, 1, 1, -3, -3, 1, 1, -3, -3 }^{T}
$t_2 =$ { 5, 1, -3, 1, 1, -3, -3, 1, -3, 1, -3, 1, -3, -3, 1, -3, 5, 1, 1, 1, 1, -3, -3, -3, -3, -3, 1, 1, -3, 1, -7, 1, 5, -3, 1, -7, 5, 5, 5, 1, 1, 1, -3, 1, -3, 1, 1, -7, 1, 1, -7, 5, 1, 1, 5, 1, -3, -3, 5, 1, -3, -3, 5 }^{T}

$$ {}_{13}\mathcal{M} = \begin{pmatrix} \begin{bmatrix}0\\t_0\end{bmatrix} & \begin{bmatrix}0\\t_1\end{bmatrix} & \begin{bmatrix}0\\t_2\end{bmatrix} & \begin{bmatrix}0\\t_1\end{bmatrix} & \begin{bmatrix}0\\t_2\end{bmatrix} \\ \begin{bmatrix}0\\t_1\end{bmatrix} & \begin{bmatrix}26\\t_0\end{bmatrix} & \begin{bmatrix}51\\t_1\end{bmatrix} & \begin{bmatrix}38\\t_2\end{bmatrix} & \begin{bmatrix}13\\t_2\end{bmatrix} \\ \begin{bmatrix}0\\t_2\end{bmatrix} & \begin{bmatrix}51\\t_1\end{bmatrix} & \begin{bmatrix}39\\t_0\end{bmatrix} & \begin{bmatrix}13\\t_2\end{bmatrix} & \begin{bmatrix}26\\t_1\end{bmatrix} \\ \begin{bmatrix}0\\t_1\end{bmatrix} & \begin{bmatrix}38\\t_2\end{bmatrix} & \begin{bmatrix}13\\t_2\end{bmatrix} & \begin{bmatrix}26\\t_0\end{bmatrix} & \begin{bmatrix}51\\t_1\end{bmatrix} \\ \begin{bmatrix}0\\t_2\end{bmatrix} & \begin{bmatrix}13\\t_2\end{bmatrix} & \begin{bmatrix}26\\t_1\end{bmatrix} & \begin{bmatrix}51\\t_1\end{bmatrix} & \begin{bmatrix}39\\t_0\end{bmatrix} \end{pmatrix} $$

Representative elements for rows of ${}_{13}\mathcal{H}$ are in the order: 0, 3, 5, 15, 17, 51, 85, 255, 33, 99, 165, 495, 547, 1331, 2735, 1023, 9, 27, 45, 119, 153, 427, 765, 231, 297, 891, 843, 1501, 1655, 1363, 2815, 63, 65, 195, 325, 975, 581, 1743, 693, 2015, 323, 655, 633, 717, 1879, 1343, 189, 455, 585, 1755, 2779, 3519, 219, 365, 951, 1179, 2907, 3567, 795, 1325, 3823, 819, 1365, 4095, 489, 571, 1235, 2775, 2031, 197, 335, 573, 921, 1195, 2943, 123, 141, 407, 697, 1439, 373, 927, 293, 879, 603, 1773, 1771, 1963, 1013, 249, 267, 797, 1253, 1517, 887, 1203, 2743, 2043, 53, 95, 225, 291, 869, 1455, 751, 627, 1357, 3007, 243, 277, 831, 149, 447, 139, 413, 679, 1277, 237, 311, 857, 1515, 983, 969, 729, 1899, 1781, 1003, 347, 1005, 441, 715, 1885, 1871, 669, 1853, 933, 1263, 723, 1909, 1661, 469, 639, 77, 215, 377, 711, 1181, 1901, 1757, 1883, 1973, 893, 459, 605, 1767, 1323, 3039, 483, 549, 1647, 683, 2045, 29, 39, 105, 187, 461, 599, 1247, 363, 957, 915, 1205, 3551, 435, 725, 1919, 83, 245, 287, 281, 811, 1405, 479, 275, 821, 1375, 383, 71, 201, 303, 567, 1227, 2795, 1983, 163, 485, 559, 615, 1237, 3067, 111, 177, 467, 629, 1695, 349, 999, 329, 987, 873, 1467, 1723, 1711, 703, 159, 269, 739, 1191, 1469, 955, 1229, 2747, 1791, 43, 125, 135, 393, 667, 1965, 989, 825, 1355, 3063, 207, 337, 1011, 169, 507, 209, 371, 917, 1215, 183, 473, 619, 1725, 943, 591, 621, 1719, 1403, 863, 437, 735, 315, 845, 1495, 1487, 741, 1511, 663, 1271, 813, 1399, 1523, 343, 1017, 89, 235, 317, 839, 1175, 1463, 1499, 1751, 1391, 763, 423, 745, 1851, 1333, 3055, 399, 553, 1659, 853, 1535, 23, 57, 75, 221, 359, 937, 1275, 429, 759, 807, 1197, 3575, 411, 685, 2039, 101, 175, 497, 305, 851, 1525, 503, 401, 691, 2005, 509, 113, 147.

Representative elements for columns of ${}_{13}\mathcal{H}$ are in the order: 0, 1365, 819, 3823, 1325, 795, 3567, 2907, 1179, 951, 365, 219, 3519, 2779, 1755, 585, 455, 189, 1343, 1879, 717, 633, 655, 323, 2015, 693, 1743, 581, 975, 325, 195, 65, 63, 2815, 1363, 1655, 1501, 843, 891, 297, 231, 765, 427, 153, 119, 45, 27, 9, 1023, 2735, 1331, 547, 495, 165, 99, 33, 255, 85, 51, 17, 15, 5, 3, 4095, 1781, 1899, 729, 969, 983, 1515, 857, 311, 237, 1277, 679, 413, 139, 447, 149, 831, 277, 243, 3007, 1357, 627, 751, 1455, 869, 291, 225, 95, 53, 2043, 2743, 1203, 887, 1517, 1253, 797, 267, 249, 1013, 1963, 1771, 1773, 603, 879, 293, 927, 373, 1439, 697, 407, 141, 123, 2943, 1195, 921, 573, 335, 197, 2031, 2775, 1235, 571, 489, 1003, 71, 383, 1375, 821, 275, 479, 1405, 811, 281, 287, 245, 83, 1919, 725, 435, 3551, 1205, 915, 957, 363, 1247, 599, 461, 187, 105, 39, 29, 2045, 683, 1647, 549, 483, 3039, 1323, 1767, 605, 459, 893, 1973, 1883, 1757, 1901, 1181, 711, 377, 215, 77, 639, 469, 1661, 1909, 723, 1263, 933, 1853, 669, 1871, 1885, 715, 441, 1005, 347, 201, 1403, 1719, 621, 591, 943, 1725, 619, 473, 183, 1215, 917, 371, 209, 507, 169, 1011, 337, 207, 3063, 1355, 825, 989, 1965, 667, 393, 135, 125, 43, 1791, 2747, 1229, 955, 1469, 1191, 739, 269, 159, 703, 1711, 1723, 1467, 873, 987, 329, 999, 349, 1695, 629, 467, 177, 111, 3067, 1237, 615, 559, 485, 163, 1983, 2795, 1227, 567, 303, 863, 113, 509, 2005, 691, 401, 503, 1525, 851, 305, 497, 175, 101, 2039, 685, 411, 3575, 1197, 807, 759, 429, 1275, 937, 359, 221, 75, 57, 23, 1535, 853, 1659, 553, 399, 3055, 1333, 1851, 745, 423, 763, 1391, 1751, 1499, 1463, 1175, 839, 317, 235, 89, 1017, 343, 1523, 1399, 813, 1271, 663, 1511, 741, 1487, 1495, 845, 315, 735, 437, 147.

Appendix B3: The structure of ${}_{19}\mathcal{M}$

${}_{19}\mathcal{M}$ is of size 27×27, $g_{19} = 27596$. The number of different vectors is 13, their size is 511.

${}_{19}\mathcal{M} =$

$[0; t_{0}]$	$[0; t_{1}]$	$[0; t_{2}]$	$[0; t_{3}]$	$[0; t_{4}]$	$[0; t_{5}]$	$[0; t_{6}]$	$[0; t_{7}]$	$[0; t_{8}]$	$[0; t_{9}]$	$[0; t_{10}]$	$[0; t_{11}]$	$[0; t_{12}]$	$[0; t_{13}]$	$[0; t_{1}]$	$[0; t_{2}]$	$[0; t_{3}]$	$[0; t_{4}]$	$[0; t_{5}]$	$[0; t_{6}]$	$[0; t_{7}]$	$[0; t_{8}]$	$[0; t_{9}]$	$[0; t_{10}]$	$[0; t_{11}]$	$[0; t_{12}]$	$[0; t_{13}]$
$[0; t_{1}]$	$[467; t_{0}]$	$[489; t_{2}]$	$[155; t_{4}]$	$[312; t_{3}]$	$[326; t_{8}]$	$[85; t_{4}]$	$[421; t_{9}]$	$[141; t_{5}]$	$[326; t_{3}]$	$[232; t_{11}]$	$[20; t_{7}]$	$[313; t_{2}]$	$[459; t_{1}]$	$[8; t_{13}]$	$[154; t_{12}]$	$[141; t_{9}]$	$[382; t_{6}]$	$[328; t_{13}]$	$[226; t_{8}]$	$[447; t_{11}]$	$[241; t_{6}]$	$[46; t_{7}]$	$[330; t_{12}]$	$[235; t_{10}]$	$[137; t_{10}]$	$[139; t_{5}]$
$[0; t_{2}]$	$[489; t_{2}]$	$[314; t_{0}]$	$[157; t_{3}]$	$[491; t_{3}]$	$[376; t_{11}]$	$[250; t_{9}]$	$[507; t_{6}]$	$[28; t_{11}]$	$[171; t_{4}]$	$[192; t_{5}]$	$[286; t_{8}]$	$[160; t_{1}]$	$[124; t_{12}]$	$[154; t_{12}]$	$[336; t_{1}]$	$[334; t_{4}]$	$[143; t_{9}]$	$[122; t_{10}]$	$[318; t_{7}]$	$[244; t_{8}]$	$[70; t_{7}]$	$[64; t_{6}]$	$[31; t_{13}]$	$[449; t_{5}]$	$[190; t_{13}]$	$[283; t_{10}]$
$[0; t_{3}]$	$[155; t_{4}]$	$[157; t_{3}]$	$[25; t_{0}]$	$[202; t_{2}]$	$[487; t_{11}]$	$[485; t_{12}]$	$[357; t_{13}]$	$[431; t_{5}]$	$[395; t_{1}]$	$[140; t_{8}]$	$[49; t_{5}]$	$[144; t_{9}]$	$[18; t_{6}]$	$[141; t_{9}]$	$[334; t_{4}]$	$[379; t_{2}]$	$[381; t_{1}]$	$[105; t_{8}]$	$[7; t_{13}]$	$[483; t_{10}]$	$[396; t_{10}]$	$[392; t_{12}]$	$[53; t_{7}]$	$[268; t_{11}]$	$[51; t_{6}]$	$[179; t_{7}]$
$[0; t_{4}]$	$[312; t_{3}]$	$[491; t_{3}]$	$[202; t_{2}]$	$[182; t_{0}]$	$[91; t_{5}]$	$[311; t_{1}]$	$[147; t_{12}]$	$[473; t_{11}]$	$[39; t_{2}]$	$[345; t_{11}]$	$[348; t_{10}]$	$[492; t_{4}]$	$[445; t_{9}]$	$[382; t_{6}]$	$[143; t_{9}]$	$[381; t_{1}]$	$[201; t_{12}]$	$[352; t_{7}]$	$[467; t_{10}]$	$[341; t_{5}]$	$[93; t_{13}]$	$[248; t_{13}]$	$[226; t_{6}]$	$[220; t_{8}]$	$[35; t_{7}]$	$[89; t_{8}]$
$[0; t_{5}]$	$[326; t_{8}]$	$[376; t_{11}]$	$[487; t_{11}]$	$[91; t_{5}]$	$[85; t_{0}]$	$[37; t_{13}]$	$[354; t_{12}]$	$[491; t_{3}]$	$[70; t_{10}]$	$[474; t_{2}]$	$[220; t_{2}]$	$[242; t_{7}]$	$[48; t_{6}]$	$[328; t_{13}]$	$[122; t_{10}]$	$[105; t_{8}]$	$[352; t_{7}]$	$[505; t_{4}]$	$[391; t_{9}]$	$[244; t_{4}]$	$[270; t_{1}]$	$[205; t_{6}]$	$[15; t_{9}]$	$[109; t_{3}]$	$[298; t_{12}]$	$[268; t_{1}]$
$[0; t_{6}]$	$[85; t_{4}]$	$[250; t_{9}]$	$[485; t_{12}]$	$[311; t_{1}]$	$[37; t_{13}]$	$[396; t_{0}]$	$[78; t_{2}]$	$[111; t_{7}]$	$[146; t_{2}]$	$[198; t_{10}]$	$[296; t_{12}]$	$[422; t_{3}]$	$[389; t_{3}]$	$[226; t_{8}]$	$[318; t_{7}]$	$[7; t_{13}]$	$[467; t_{10}]$	$[391; t_{9}]$	$[317; t_{11}]$	$[285; t_{8}]$	$[170; t_{1}]$	$[5; t_{5}]$	$[440; t_{4}]$	$[79; t_{6}]$	$[100; t_{11}]$	$[359; t_{5}]$
$[0; t_{7}]$	$[421; t_{9}]$	$[507; t_{6}]$	$[357; t_{13}]$	$[147; t_{12}]$	$[354; t_{12}]$	$[78; t_{2}]$	$[74; t_{0}]$	$[300; t_{6}]$	$[164; t_{1}]$	$[422; t_{13}]$	$[138; t_{1}]$	$[438; t_{4}]$	$[228; t_{3}]$	$[447; t_{11}]$	$[244; t_{8}]$	$[483; t_{10}]$	$[341; t_{5}]$	$[244; t_{4}]$	$[285; t_{8}]$	$[37; t_{7}]$	$[341; t_{2}]$	$[63; t_{11}]$	$[102; t_{3}]$	$[11; t_{9}]$	$[231; t_{5}]$	$[163; t_{10}]$
$[0; t_{8}]$	$[141; t_{5}]$	$[28; t_{11}]$	$[431; t_{5}]$	$[473; t_{11}]$	$[491; t_{3}]$	$[111; t_{7}]$	$[300; t_{6}]$	$[411; t_{0}]$	$[105; t_{8}]$	$[15; t_{3}]$	$[449; t_{4}]$	$[109; t_{10}]$	$[461; t_{13}]$	$[241; t_{6}]$	$[70; t_{7}]$	$[396; t_{10}]$	$[93; t_{13}]$	$[270; t_{1}]$	$[170; t_{1}]$	$[341; t_{2}]$	$[306; t_{9}]$	$[74; t_{12}]$	$[302; t_{12}]$	$[383; t_{2}]$	$[337; t_{9}]$	$[318; t_{4}]$
$[0; t_{9}]$	$[326; t_{3}]$	$[171; t_{4}]$	$[395; t_{1}]$	$[39; t_{2}]$	$[70; t_{10}]$	$[146; t_{2}]$	$[164; t_{1}]$	$[105; t_{8}]$	$[210; t_{0}]$	$[140; t_{5}]$	$[236; t_{13}]$	$[329; t_{3}]$	$[473; t_{4}]$	$[46; t_{7}]$	$[64; t_{6}]$	$[392; t_{12}]$	$[248; t_{13}]$	$[205; t_{6}]$	$[5; t_{5}]$	$[63; t_{11}]$	$[74; t_{12}]$	$[388; t_{10}]$	$[333; t_{9}]$	$[147; t_{7}]$	$[136; t_{8}]$	$[485; t_{11}]$
$[0; t_{10}]$	$[232; t_{11}]$	$[192; t_{5}]$	$[140; t_{8}]$	$[345; t_{11}]$	$[474; t_{2}]$	$[198; t_{10}]$	$[422; t_{13}]$	$[15; t_{3}]$	$[140; t_{5}]$	$[155; t_{0}]$	$[434; t_{1}]$	$[364; t_{8}]$	$[244; t_{7}]$	$[330; t_{12}]$	$[31; t_{13}]$	$[53; t_{7}]$	$[226; t_{6}]$	$[15; t_{9}]$	$[440; t_{4}]$	$[102; t_{3}]$	$[302; t_{12}]$	$[333; t_{9}]$	$[468; t_{6}]$	$[321; t_{4}]$	$[336; t_{1}]$	$[124; t_{2}]$
$[0; t_{11}]$	$[20; t_{7}]$	$[286; t_{8}]$	$[49; t_{5}]$	$[348; t_{10}]$	$[220; t_{2}]$	$[296; t_{12}]$	$[138; t_{1}]$	$[449; t_{4}]$	$[236; t_{13}]$	$[434; t_{1}]$	$[158; t_{0}]$	$[373; t_{6}]$	$[433; t_{9}]$	$[235; t_{10}]$	$[449; t_{5}]$	$[268; t_{11}]$	$[220; t_{8}]$	$[109; t_{3}]$	$[79; t_{6}]$	$[11; t_{9}]$	$[383; t_{2}]$	$[147; t_{7}]$	$[321; t_{4}]$	$[401; t_{3}]$	$[112; t_{13}]$	$[46; t_{12}]$
$[0; t_{12}]$	$[313; t_{2}]$	$[160; t_{1}]$	$[144; t_{9}]$	$[492; t_{4}]$	$[242; t_{7}]$	$[422; t_{3}]$	$[438; t_{4}]$	$[109; t_{10}]$	$[329; t_{3}]$	$[364; t_{8}]$	$[373; t_{6}]$	$[473; t_{0}]$	$[283; t_{2}]$	$[137; t_{10}]$	$[190; t_{13}]$	$[51; t_{6}]$	$[35; t_{7}]$	$[298; t_{12}]$	$[100; t_{11}]$	$[231; t_{5}]$	$[337; t_{9}]$	$[136; t_{8}]$	$[336; t_{1}]$	$[112; t_{13}]$	$[175; t_{5}]$	$[361; t_{11}]$
$[0; t_{13}]$	$[459; t_{1}]$	$[124; t_{12}]$	$[18; t_{6}]$	$[445; t_{9}]$	$[48; t_{6}]$	$[389; t_{3}]$	$[228; t_{3}]$	$[461; t_{13}]$	$[473; t_{4}]$	$[244; t_{7}]$	$[433; t_{9}]$	$[283; t_{2}]$	$[407; t_{0}]$	$[139; t_{5}]$	$[283; t_{10}]$	$[179; t_{7}]$	$[89; t_{8}]$	$[268; t_{1}]$	$[359; t_{5}]$	$[163; t_{10}]$	$[318; t_{4}]$	$[485; t_{11}]$	$[124; t_{2}]$	$[46; t_{12}]$	$[361; t_{11}]$	$[457; t_{8}]$
$[0; t_{1}]$	$[8; t_{13}]$	$[154; t_{12}]$	$[141; t_{9}]$	$[382; t_{6}]$	$[328; t_{13}]$	$[226; t_{8}]$	$[447; t_{11}]$	$[241; t_{6}]$	$[46; t_{7}]$	$[330; t_{12}]$	$[235; t_{10}]$	$[137; t_{10}]$	$[139; t_{5}]$	$[467; t_{0}]$	$[489; t_{2}]$	$[155; t_{4}]$	$[312; t_{3}]$	$[326; t_{8}]$	$[85; t_{4}]$	$[421; t_{9}]$	$[141; t_{5}]$	$[326; t_{3}]$	$[232; t_{11}]$	$[20; t_{7}]$	$[313; t_{2}]$	$[459; t_{1}]$
$[0; t_{2}]$	$[154; t_{12}]$	$[336; t_{1}]$	$[334; t_{4}]$	$[143; t_{9}]$	$[122; t_{10}]$	$[318; t_{7}]$	$[244; t_{8}]$	$[70; t_{7}]$	$[64; t_{6}]$	$[31; t_{13}]$	$[449; t_{5}]$	$[190; t_{13}]$	$[283; t_{10}]$	$[489; t_{2}]$	$[314; t_{0}]$	$[157; t_{3}]$	$[491; t_{3}]$	$[376; t_{11}]$	$[250; t_{9}]$	$[507; t_{6}]$	$[28; t_{11}]$	$[171; t_{4}]$	$[192; t_{5}]$	$[286; t_{8}]$	$[160; t_{1}]$	$[124; t_{12}]$
$[0; t_{3}]$	$[141; t_{9}]$	$[334; t_{4}]$	$[379; t_{2}]$	$[381; t_{1}]$	$[105; t_{8}]$	$[7; t_{13}]$	$[483; t_{10}]$	$[396; t_{10}]$	$[392; t_{12}]$	$[53; t_{7}]$	$[268; t_{11}]$	$[51; t_{6}]$	$[179; t_{7}]$	$[155; t_{4}]$	$[157; t_{3}]$	$[25; t_{0}]$	$[202; t_{2}]$	$[487; t_{11}]$	$[485; t_{12}]$	$[357; t_{13}]$	$[431; t_{5}]$	$[395; t_{1}]$	$[140; t_{8}]$	$[49; t_{5}]$	$[144; t_{9}]$	$[18; t_{6}]$
$[0; t_{4}]$	$[382; t_{6}]$	$[143; t_{9}]$	$[381; t_{1}]$	$[201; t_{12}]$	$[352; t_{7}]$	$[467; t_{10}]$	$[341; t_{5}]$	$[93; t_{13}]$	$[248; t_{13}]$	$[226; t_{6}]$	$[220; t_{8}]$	$[35; t_{7}]$	$[89; t_{8}]$	$[312; t_{3}]$	$[491; t_{3}]$	$[202; t_{2}]$	$[182; t_{0}]$	$[91; t_{5}]$	$[311; t_{1}]$	$[147; t_{12}]$	$[473; t_{11}]$	$[39; t_{2}]$	$[345; t_{11}]$	$[348; t_{10}]$	$[492; t_{4}]$	$[445; t_{9}]$
$[0; t_{5}]$	$[328; t_{13}]$	$[122; t_{10}]$	$[105; t_{8}]$	$[352; t_{7}]$	$[505; t_{4}]$	$[391; t_{9}]$	$[244; t_{4}]$	$[270; t_{1}]$	$[205; t_{6}]$	$[15; t_{9}]$	$[109; t_{3}]$	$[298; t_{12}]$	$[268; t_{1}]$	$[326; t_{8}]$	$[376; t_{11}]$	$[487; t_{11}]$	$[91; t_{5}]$	$[85; t_{0}]$	$[37; t_{13}]$	$[354; t_{12}]$	$[491; t_{3}]$	$[70; t_{10}]$	$[474; t_{2}]$	$[220; t_{2}]$	$[242; t_{7}]$	$[48; t_{6}]$
$[0; t_{6}]$	$[226; t_{8}]$	$[318; t_{7}]$	$[7; t_{13}]$	$[467; t_{10}]$	$[391; t_{9}]$	$[317; t_{11}]$	$[285; t_{8}]$	$[170; t_{1}]$	$[5; t_{5}]$	$[440; t_{4}]$	$[79; t_{6}]$	$[100; t_{11}]$	$[359; t_{5}]$	$[85; t_{4}]$	$[250; t_{9}]$	$[485; t_{12}]$	$[311; t_{1}]$	$[37; t_{13}]$	$[396; t_{0}]$	$[78; t_{2}]$	$[111; t_{7}]$	$[146; t_{2}]$	$[198; t_{10}]$	$[296; t_{12}]$	$[422; t_{3}]$	$[389; t_{3}]$
$[0; t_{7}]$	$[447; t_{11}]$	$[244; t_{8}]$	$[483; t_{10}]$	$[341; t_{5}]$	$[244; t_{4}]$	$[285; t_{8}]$	$[37; t_{7}]$	$[341; t_{2}]$	$[63; t_{11}]$	$[102; t_{3}]$	$[11; t_{9}]$	$[231; t_{5}]$	$[163; t_{10}]$	$[421; t_{9}]$	$[507; t_{6}]$	$[357; t_{13}]$	$[147; t_{12}]$	$[354; t_{12}]$	$[78; t_{2}]$	$[74; t_{0}]$	$[300; t_{6}]$	$[164; t_{1}]$	$[422; t_{13}]$	$[138; t_{1}]$	$[438; t_{4}]$	$[228; t_{3}]$
$[0; t_{8}]$	$[241; t_{6}]$	$[70; t_{7}]$	$[396; t_{10}]$	$[93; t_{13}]$	$[270; t_{1}]$	$[170; t_{1}]$	$[341; t_{2}]$	$[306; t_{9}]$	$[74; t_{12}]$	$[302; t_{12}]$	$[383; t_{2}]$	$[337; t_{9}]$	$[318; t_{4}]$	$[141; t_{5}]$	$[28; t_{11}]$	$[431; t_{5}]$	$[473; t_{11}]$	$[491; t_{3}]$	$[111; t_{7}]$	$[300; t_{6}]$	$[411; t_{0}]$	$[105; t_{8}]$	$[15; t_{3}]$	$[449; t_{4}]$	$[109; t_{10}]$	$[461; t_{13}]$
$[0; t_{9}]$	$[46; t_{7}]$	$[64; t_{6}]$	$[392; t_{12}]$	$[248; t_{13}]$	$[205; t_{6}]$	$[5; t_{5}]$	$[63; t_{11}]$	$[74; t_{12}]$	$[388; t_{10}]$	$[333; t_{9}]$	$[147; t_{7}]$	$[136; t_{8}]$	$[485; t_{11}]$	$[326; t_{3}]$	$[171; t_{4}]$	$[395; t_{1}]$	$[39; t_{2}]$	$[70; t_{10}]$	$[146; t_{2}]$	$[164; t_{1}]$	$[105; t_{8}]$	$[210; t_{0}]$	$[140; t_{5}]$	$[236; t_{13}]$	$[329; t_{3}]$	$[473; t_{4}]$
$[0; t_{10}]$	$[330; t_{12}]$	$[31; t_{13}]$	$[53; t_{7}]$	$[226; t_{6}]$	$[15; t_{9}]$	$[440; t_{4}]$	$[102; t_{3}]$	$[302; t_{12}]$	$[333; t_{9}]$	$[468; t_{6}]$	$[321; t_{4}]$	$[336; t_{1}]$	$[124; t_{2}]$	$[232; t_{11}]$	$[192; t_{5}]$	$[140; t_{8}]$	$[345; t_{11}]$	$[474; t_{2}]$	$[198; t_{10}]$	$[422; t_{13}]$	$[15; t_{3}]$	$[140; t_{5}]$	$[155; t_{0}]$	$[434; t_{1}]$	$[364; t_{8}]$	$[244; t_{7}]$
$[0; t_{11}]$	$[235; t_{10}]$	$[449; t_{5}]$	$[268; t_{11}]$	$[220; t_{8}]$	$[109; t_{3}]$	$[79; t_{6}]$	$[11; t_{9}]$	$[383; t_{2}]$	$[147; t_{7}]$	$[321; t_{4}]$	$[401; t_{3}]$	$[112; t_{13}]$	$[46; t_{12}]$	$[20; t_{7}]$	$[286; t_{8}]$	$[49; t_{5}]$	$[348; t_{10}]$	$[220; t_{2}]$	$[296; t_{12}]$	$[138; t_{1}]$	$[449; t_{4}]$	$[236; t_{13}]$	$[434; t_{1}]$	$[158; t_{0}]$	$[373; t_{6}]$	$[433; t_{9}]$
$[0; t_{12}]$	$[137; t_{10}]$	$[190; t_{13}]$	$[51; t_{6}]$	$[35; t_{7}]$	$[298; t_{12}]$	$[100; t_{11}]$	$[231; t_{5}]$	$[337; t_{9}]$	$[136; t_{8}]$	$[336; t_{1}]$	$[112; t_{13}]$	$[175; t_{5}]$	$[361; t_{11}]$	$[313; t_{2}]$	$[160; t_{1}]$	$[144; t_{9}]$	$[492; t_{4}]$	$[242; t_{7}]$	$[422; t_{3}]$	$[438; t_{4}]$	$[109; t_{10}]$	$[329; t_{3}]$	$[364; t_{8}]$	$[373; t_{6}]$	$[473; t_{0}]$	$[283; t_{2}]$
$[0; t_{13}]$	$[139; t_{5}]$	$[283; t_{10}]$	$[179; t_{7}]$	$[89; t_{8}]$	$[268; t_{1}]$	$[359; t_{5}]$	$[163; t_{10}]$	$[318; t_{4}]$	$[485; t_{11}]$	$[124; t_{2}]$	$[46; t_{12}]$	$[361; t_{11}]$	$[457; t_{8}]$	$[459; t_{1}]$	$[124; t_{12}]$	$[18; t_{6}]$	$[445; t_{9}]$	$[48; t_{6}]$	$[389; t_{3}]$	$[228; t_{3}]$	$[461; t_{13}]$	$[473; t_{4}]$	$[244; t_{7}]$	$[433; t_{9}]$	$[283; t_{2}]$	$[407; t_{0}]$