THE WEIGHT RECURSIONS FOR THE 2-ROTATION
SYMMETRIC QUARTIC BOOLEAN FUNCTIONS

THOMAS W. CUSICK
Department of Mathematics
University at Buffalo
244 Mathematics Bldg., Buffalo, NY 14260

YOUNHWAN CHEON
Department of Military Operations Research
Korea Army Academy at YeongCheon
135-9, Hoguk-ro, Gogyeong-myeon, Yeongcheon-si, Gyeongsangbuk-do, Republic of Korea, 38900

(Communicated by Claude Carlet)

Abstract. A Boolean function in \( n \) variables is 2-rotation symmetric if it is invariant under even powers of \( \rho(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1) \), but not under the first power (ordinary rotation symmetry); we call such a function a 2-function. A 2-function is called monomial rotation symmetric (MRS) if it is generated by applying powers of \( \rho^2 \) to a single monomial. If the quartic MRS 2-function in \( 2n \) variables has a monomial \( x_1x_qx_rx_s \), then we use the notation \( 2-(1,q,r,s)_{2n} \) for the function. A detailed theory of equivalence of quartic MRS 2-functions in \( 2n \) variables was given in a 2020 paper by Cusick, Cheon and Dougan. This theory divides naturally into two classes, called \( mf_1 \) and \( mf_2 \) in the paper. After describing the equivalence classes, the second major problem is giving details of the linear recursions that the Hamming weights for any sequence of functions \( 2-(1,q,r,s)_{2n} \) (with \( q < r < s \), say), \( n = s, s + 1, \ldots \) can be shown to satisfy. This problem was solved for the \( mf_1 \) case only in the 2020 paper. Using new ideas about “short” functions, Cusick and Cheon found formulas for the \( mf_2 \) weights in a 2021 sequel to the 2020 paper. In this paper the actual recursions for the weights in the \( mf_2 \) case are determined.

1. Introduction

A Boolean function \( f \) is said to be rotation symmetric (RS) if the algebraic normal form of the functions is unchanged by any cyclic permutation of the variables \( \rho(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1) \). The function is said to be \( k \)-rotation symmetric (k-RS) if it is invariant under the \( k \)th power of \( \rho \) but not under any smaller power (so the number of variables must be divisible by \( k \)). A \( k \)-rotation symmetric function is said to be \( k \)-monomial rotation symmetric (k-MRS) if it is generated by applying powers of \( \rho^k \) to a single monomial. We say that two Boolean functions \( f(\vec{x}) \) and \( g(\vec{x}) \) in \( B_n \) are affine equivalent if \( g(\vec{x}) = f(A\vec{x} + \vec{b}) \), where \( A \) is an \( n \) by \( n \) nonsingular matrix over the finite field \( GF(2) \) and \( b \) is an \( n \)-vector over \( GF(2) \). We say \( f(A\vec{x} + \vec{b}) \) is a nonsingular affine transformation of \( f(\vec{x}) \). If \( k = 1 \), we simply say that the function is MRS, and in general we use the abbreviations RS for rotation symmetric and MRS for monomial rotation symmetric.

2020 Mathematics Subject Classification: 94C10 94A60 06E30.

Key words and phrases: Boolean function, quartic, rotation symmetric, affine equivalence, Hamming weight, cryptography.
The 2-RS functions were introduced in [10], which gives an application of these functions to the well known problem of finding Boolean functions of high nonlinearity. Further applications of the \(k\)-rotation symmetric functions \((k \geq 2)\) to coding theory and S-box design were given in [10, 11, 12, 13, 14]. The 2-RS functions are used in [1] in the construction of bent and semi-bent RS functions.

After earlier work on special cases, it was proved in [3] that for any RS function \(f_k(x_1, x_2, \ldots, x_k)\) in \(k\) variables the sequence of weights \(wt(f_k)\) satisfies a homogeneous linear recursion with integer coefficients. In the case \(k = 2\) of quadratic functions, this result was useful [2] in giving an explicit new method for solving the notorious problem of deciding exactly which quadratic RS functions are balanced. It is to be expected that the recursions for higher degree RS functions will lead to further useful theorems.

2. Preliminaries

The standard form of a quartic 2-MRS function in \(2n\) variables is given by

\[
2-f(x_1, x_r, x_s, x_t)_{2n} = x_1 x_r x_s x_t + x_3 x_r+2 x_s+2 x_t+2 + \ldots + x_{2n-1} x_r-2 x_s-2 x_t-2
\]

where \(1 < r < s < t\).

We recall some general definitions needed for this paper from [6].

**Definition 1. MRS function notation** We use the notation \([a, b, c]\) for the cubic monomial \(x_a x_b x_c\), with a similar notation for monomials of other degrees. We use the notation \((a, b, c, d)\) for a quartic MRS function in \(k\) variables one of whose monomials is \([a, b, c, d]\), and the notation \(2-(a, b, c, d)\) for a quartic 2-MRS function in \(k\) variables, with similar notation for other degrees. We do not require that the integers be arranged in increasing order, since it is sometimes convenient to use other orderings in the statements of some of our results. For example, the function in (1) would be denoted by \(2-(1, r, s, t)_{2n}\). If the number of variables is clear from the context, we will often omit it in the notation. If we want to emphasize that a function is simply MRS, rather than 2-MRS, we will call the function an *ordinary* MRS function.

**Definition 2. Short functions.** If \(n\) is even, it is possible for the representation (1) to contain only \(n/2\) or \(n/4\) distinct terms (see [4, p. 193]). If this happens, we modify the definition of the 2-function in (1) so that only the distinct terms are used. We define the “short quartic 2-functions” to be the ones with fewer than \(n\) terms. If \(n\) is divisible by 4 and the 2-function has \(n/4\) terms, we say it is a “very short” function. If the 2-function in (1) has \(n\) terms, we say the function is *nonshort*.

**Definition 3. Pure and mixed forms.** A monomial (or function) which contains only odd or only even integers is said to be *pure form*. A monomial that is not pure form is said to be *mixed form*.

**Definition 4. Type 1, Type 2 mixed form functions.** A quartic 2-function whose defining monomial contains exactly one or exactly three odd integers is called a *type 1 mixed form (mf1) function*. A nonshort quartic 2-function whose defining monomial contains exactly two even integers (and thus, two odd integers) is called a *type 2 mixed form (mf2) function*.

In this paper all the new results are for the \(mf2\) functions.
Definition 5. Quadratic 2-functions Suppose we have a quadratic 2-function
\[ x_1 x_a + x_2 x_{a+1} + \ldots + x_{2n-1} x_{a+2n-2} \]
in 2n variables, where all indices of variables are reduced mod(2n). We use the notation 2-(1, a)2n for this function or, for brevity, 2-(1, a), when the number of variables is understood. More generally, given any quadratic 2-function in 2n variables which contains a monomial \(x_r x_s\) we may use the notations 2-(r, s)2n or 2-(r, s). In particular, we must use this more general notation in the cases where all indices in the variables are even, so \(x_1\) does not appear in the function.

Definition 6. \(\mu\)-values. Let 2-(a, b) be a quadratic 2-function. Then we define \(\mu = b - a\) to be the \(\mu\)-value for 2-(a, b).

Definition 7. Chi values and chi pairs. Let \(f = 2-(1, a, b, c)_{2n}\), where a odd and b, c even (mod 2n), and let \(\chi_1 = a - 1\) (mod 2n), \(\chi_2 = c - b\) (mod 2n). Then the \(\chi\) values of \(f\) are the members of the unordered pair \(\{\chi_1, \chi_2\}\) (duplicate values are possible). We define \(\chi = \{\chi_1, \chi_2\}\), and we say \(\chi\) is the chi pair for \(f\).

Later in the paper we need some results which follow immediately from the following theorem in the paper [6]. We state these results here to separate them from the new work later in this paper.

Theorem 1. [6, Th. 6, p. 366] If \(f\) and \(g\) are \(mf2\) quartic 2-MRS functions, then \(f\) and \(g\) are equivalent by a permutation which preserves 2-rotation symmetry if and only if the \(\chi\) values of \(g\) are \(\{k\chi_1, k\chi_2, 2n - k\chi_2, 2n - k\chi_1, k\chi_1, k\chi_2\}\) or \(\{2n - k\chi_1, 2n - k\chi_2\}\), where \(gcd(k, n) = 1\), and \(\{\chi_1, \chi_2\}\) are the \(\chi\) values of \(f\).

Corollary 1. Suppose \(f\) is an \(mf2\) quartic 2-MRS function with \(\chi_f = \{2, 2\}\), and \(g\) is a quartic 2-MRS function with \(\chi_g = k\{2, 2\}\). Then
\[ wt(f) = wt(g) \text{ if and only if } gcd(n, k) = 1. \]

Example 1. For \(n = 7\), we have \(wt((1, 2, 3, 4)_{14}) = wt((1, 2, 5, 6)_{14}) = wt((1, 2, 7, 8)_{14}) = wt((1, 2, 11, 12)_{14}) = 3, 928\), but \(wt((1, 2, 15, 16)_{14}) = 8, 128\). For \(n = 10\), we have \(wt((1, 2, 3, 4)_{20}) = wt((1, 2, 7, 8)_{20}) = 316, 800\), but \(wt((1, 2, 9, 10)_{20}) = 324, 576 = wt((1, 2, 5, 6)_{20})\).

Corollary 2. Define the functions \(b_{n,i} = 2-(1, 2, i, 3i - 1)_{2n}\), with \(n \geq 2i + 1\). The functions \(b_{n,3}\) with \(\chi = \{2, 6\}\) and \(b_{n, m+1}\) with \(\chi = m\{1, 3\}\) for even \(m \geq 4\) are permutation equivalent if and only if \(gcd(m, n) = 1\).

Corollary 3. Define the functions \(d_{n,i} = 2-(1, 2, i, 4i - 2)_{2n}\), with \(n \geq 2i + 1\). The functions \(d_{n,3}\) with \(\chi = \{2, 8\}\) and \(d_{n, m+1}\) with \(\chi = m\{1, 4\}\) for even \(m \geq 4\) are permutation equivalent if and only if \(gcd(m, n) = 1\).

Corollary 4. Define the functions \(u_{n, i} = 2-(1, 2, i, 5i - 3)_{2n}\), with \(n \geq 2i + 1\). The functions \(u_{n,3}\) with \(\chi = \{2, 10\}\) and \(u_{n, m+1}\) with \(\chi = m\{1, 5\}\) for even \(m \geq 4\) are permutation equivalent if and only if \(gcd(m, n) = 1\).

Corollary 5. Define the functions \(y_{n, i} = 2-(1, 2, a(i - 1) + 1, b(i - 1) + 2)_{2n}\), with \(n \geq 2i + 1\). The functions \(y_{n,3}\) with \(\chi = \{2a, 2b\}\) and \(y_{n, m+1}\) with \(\chi = m\{a, b\}\) for even \(m \geq 4\) are permutation equivalent if and only if \(gcd(m, n) = 1\).
Table 1. The recursion polynomial for $f$ corresponding to some $\mu$ values.

| $\mu$ | $p(x)$ |
|-------|--------|
| 2     | $x^3 - 4x^2 - 8x + 32 = (x - 4)(x^2 - 8)$ |
| 4     | $x^5 - 4x^4 - 64x + 256 = (x - 4)(x^4 - 64)$ |
| 6     | $x^7 - 4x^6 - 512x + 2048 = (x - 4)(x^6 - 512)$ |
| 8     | $x^9 - 4x^8 - 4096x + 16384 = (x - 4)(x^8 - 4096)$ |

$t = 1 (t \text{ is odd})$ $x^t - 4x^{t-1} - 2^{(3t-3)/2}x + 2^{(3t+1)/2} = (x - 4)(x^{t-1} - 2^{(3t-3)/2})$

3. Weight recursions for quadratic MRS functions

A general formula for the recursion polynomial of the quadratic 2-function $2-(1,t)_{2n}$ for $t$ odd is given in the following theorem.

Theorem 2. The recursion polynomial for the weights of $2-(1,t)_{2n}, t > 2$ and $t$ odd, is $x^t - 4x^{t-1} - 2^{(3t-3)/2}x + 2^{(3t+1)/2} = (x - 4)(x^{t-1} - 2^{(3t-3)/2})$. The recursion is valid for the sequence of weights $wt((1,t)_n)$ at least for all $m \geq 2t - 1$.

Proof. For $t$ odd, $2-(1,t)_{2n}$ has only odd subscript variables $x_{3j-1}$. Thus if we define $t = 2T - 1$, we can map $2-(1,1)_{2n}$ to the quadratic RS function $(1,T)_n$ in $n$ variables by replacing the odd subscripts $2j - 1$ by $j$, $1 \leq j \leq n$. We know from [2, Theorem 1] that the recursion polynomial for $(1,T)_n$ is $(x - 2)(x^{2T - 2} - 2T - 1)$, so the recursion polynomial for $2-(1,t)_{2n}$ is $(x - 4)(x^{t-1} - 2^{(3t-3)/2})$.

Lemma 1. If $f$ is a quadratic 2-MRS function, and the $\mu$ value of $f$ is even, then the recursion polynomial for $f$ is in Table 1.

Theorem 3. Let $f_n = 2-(1,t)_{2n}$ with $t$ odd, and $k = gcd(n, \frac{t-1}{2})$, we have

$$wt(f_n) = 2^n(2^{n-1} - 2^{n/2+k-1}), \text{ if } \frac{n}{k} \text{ is even, } n \neq 2k$$

$$wt(f_n) = 2^{2n-1}, \text{ otherwise.}$$

Proof. Let $f_n = 2-(1,t)_{2n} = x_1x_t + x_3x_{t+2} + \cdots + x_{2n-1}x_{t-2}$ with $t > 2$, odd. The $f_n$ is the essentially the same as the ordinary rotation symmetric function $f_{n,(t+1)/2} = x_1x_{(t+1)/2} + x_2x_{(t+1)/2+1} + \cdots + x_{2n}x_{(t+1)/2-2} - 1$ with variables $y_i = x_{2i-1}, 1 \leq i \leq n$. By [15, Th. 8], we have $wt(f_{n,(t+1)/2})$ except for the short functions that is $n = 2k$, so we have the results.

Theorem 4. The weight of $2-(1,t)_{2n}$ with $t$ even, is $2^{n-1}(2^n - 1)$.

Proof. Given $n$, the permutation $\sigma_m$ defined by $\sigma_m(j) = 2i, 1 \leq i \leq n - 1$, and $\sigma_m(j) = j$ for $j$ odd, $1 \leq j \leq 2n - 1$, maps $2-(1,2)_{2n}$ to $2-(1,2m+2)_{2n}$ for each $m$, $1 \leq m \leq n - 1$. Thus all of the functions $2-(1,t)_{2n}$ with $t$ even have the same weight, and it suffices to prove the weight of $f_n = 2-(1,2)_{2n}$ is $2^{n-1}(2^n - 1) = w_n$, say. We prove this by induction. The case $n = 1$ is trivial. Let $2-(1,2k)_{2n} = x_1x_{2k} + x_3x_{2k+2} + \cdots + x_{2n-1}x_{2k+2}$. If $x_1x_{2k} = 1$, then $f_{2k} = 1$ if and only if the other $2k - 2$ variables are chosen so that the remaining $k - 1$ monomials sum to $0$. By the induction hypothesis, there are $2^{2k-2} - w_k - 1$ choices of the monomials which sum to $0$. If $x_1x_{2k} = 0$ (three choices of the two variables give this), then $f_{2k} = 1$ if and only if the remaining monomials sum to $1$. By the induction hypothesis, there are $w_{k-1}$ choices of the monomials which sum to $1$. Hence we obtain $wt(f_k) = 2^{2k-2} - w_{k-1} + 3w_{k-1} = w_k$. \[\square\]
4. Weight recursions for quartic MRS functions

4.1. The cases χ = {χ₁, χ₂} with χ₁ = χ₂. In this section, we apply the Cusick and Padgett ideas in [8], especially the next lemma, to get the weights for the quartic cases where χ = χ₁ = χ₂ in χ = {χ₁, χ₂} and each χᵢ is an even integer.

Lemma 2. [8, Lemma 2.1, p. 394] Suppose a function f in v variables can be decomposed as g + h, where the variables of g and h are disjoint. (Without loss of generality, suppose g has variables x₁, ..., xₖ, and h has variables xₖ₊₁, ..., xᵥ.) Let h* be the function h with the index of each variable reduced by k. Let g₂ be g with domain restricted to k variables, and h₂ be h* with domain restricted to v − k variables. Then

\[ wt(f) = wt(g + h) = wt(g₂)wt(1 + h₂) + wt(1 + g₂)wt(h₂) = wt(g₂)(2^{v−k} − wt(h₂)) + (2^k − wt(g₂))wt(h₂). \]

Lemma 2 gives a convenient form of the well known direct sum of two Boolean functions. We shall use this frequently in the rest of this paper.

Lemma 3. Any two mf2 quartic MRS 2- functions in 2n variables with the same χ values have the same weight, and in fact are equivalent by a permutation which preserves 2-rotation symmetry.

Proof. This is a special case of Theorem 1. □

Definition 8. Given a mf2 2-function 2-(1, a, b, c)₂ₙ where a is odd and b, c are even, let gcd(2n, χ) = 2d (where χ is as defined above) and 2n = 2dl. We define the i-th string of 2-(1, a, b, c)₂ₙ to be the set of monomials \( Sᵢ \) such that

\[ Sᵢ = \{1 + 2i + νχ, a + 2i + νχ, b + 2i + νχ, c + 2i + νχ\} : 0 ≤ ν ≤ l − 1 \]

where \( i = 0, 1, ..., d − 1 \).

Example 2. Consider the function \( f = 2-(1, 2, 5, 6)₁₂ \). Thus, the χ-value of f is 5 − 1 = 4, gcd(2n, χ) = 4 and 4 · 3 = 12, so using Definition 8 we have 2d = 4 and \( l = 3 \). The strings are \( S₀ = \{[1, 5, 2, 6], [5, 9, 6, 10], [9, 1, 10, 2]\}, \)
\( S₁ = \{[3, 7, 4, 8], [7, 11, 8, 12], [11, 3, 12, 4]\} \).

Lemma 4. Every monomial of the mf2 2-function 2-(1, r, s, t) is in one and only one string.

Proof. It is clear that each monomial appears in at least one string, so we begin by showing that no monomial appears in more than one string. Let 2-(1, a, b, c)₂ₙ be a mf2 function such that a is odd and b, c are even. Assume that a given monomial \([p, q, v, w]\) appears in \( Sᵢ \) and \( Sⱼ \). This implies that there exist \( kᵢ \), \( kⱼ \) such that

\[ [p, q, v, w] = [1 + 2i + kᵢχ, a + 2i + kᵢχ, b + 2i + kᵢχ, c + 2i + kᵢχ] \]

and

\[ [p, q, v, w] = [1 + 2j + kⱼχ, a + 2j + kⱼχ, b + 2j + kⱼχ, c + 2j + kⱼχ] \]

and thus

\[ [1 + 2i + kᵢχ, a + 2i + kᵢχ, b + 2i + kᵢχ, c + 2i + kᵢχ] = [1 + 2j + kⱼχ, a + 2j + kⱼχ, b + 2j + kⱼχ, c + 2j + kⱼχ]. \]

It is obvious from the definition of mf2 that every variable index occurs exactly twice. we have 2 cases: (i) \( 1 + 2i + kᵢχ ≡ a + 2j + kⱼχ \) Mod \( (2n) \) and \( a + 2i + kᵢχ ≡
Given a \( \chi \)-function \( f_{2n, \chi} = 2 - (1, a, \chi + 1, \chi + a)_{2n} \) for some positive integer \( a \geq 2 \) such that \( \gcd(n, \chi/2) = d \) and \( l = n/d \), then

\[
\text{wt}(f_{2n, \chi}) = \frac{1}{2} (2^{2n} - (2^{2l} - 2 \text{wt}(h_{2l, 2}))^d),
\]

where \( h_{2l, 2} = 2 - (1, 2, 3, 4)_{2l} \).

**Proof.** We know that all \( \chi \)-functions with the same \( \chi \)-value are affine equivalent by Theorem 1. Since it is known that weight is affine-invariant, it suffices to consider only \( f_{2n, \chi} = 2 - (1, 2, \chi + 1, \chi + 2)_{2n} \) with \( \chi \) even. Recall from Definition 8 that the \( i \)-th string of quartic \( f_{2n, \chi} \) is defined to be the set of monomials \( S_i \) such that:

\[
S_i = \{(1 + 2i + \nu \chi, 2 + 2i + \nu \chi, \chi + 1 + 2i + \nu \chi, \\
\chi + 2 + 2i + \nu \chi) : \nu = 0, 1, \ldots, l - 1 \}
\]

where \( i = 0, 1, \ldots, d - 1 \). From this definition, there are \( d \) strings and the \( l \) lengths of each string. By Lemma 4, the sets of monomials that make up the \( d \) strings are all different. By the definition of the \( i \)-th string of quartic \( f_{2n, \chi} \), we can view \( f_{\chi} \) as the sum of \( d \) disjoint copies of \( h_{2l, 2} \). This can be done as follows: Let the \( i \)-th string of \( f_{\chi} \) be given by \( \{(1 + 2i, 2 + 2i, 1 + 2i + \chi, 2 + 2i + \chi, 1 + 2i + \chi, 2 + 2i + \chi), [1 + 2i + \chi, 2 + 2i + \chi, 1 + 2i + 2\chi, 2 + 2i + 2\chi], \ldots, [1 + 2i - \chi, 2 + 2i - \chi, 1 + 2i, 2 + 2i]\} \).

This string can be mapped to

\[
\{[2li + 1, 2li + 2, 2li + 3, 2li + 4], [2li + 3, 2li + 4, 2li + 5], \\
2li + 6], \ldots, [2li - 1, 2li + 2, 2li + 1, 2li + 2]\}.
\]

So the above monomials are affine equivalent to \( 2 - (1, 2, 3, 4)_{2l} \). Since \( i \) covers from 0 to \( d - 1 \), we have \( d \) copies of \( h_{2l, 2} \). Therefore, we can get the weight of \( f_{\chi} \) by

\[
\text{wt}(f_{2n, \chi}) = \text{wt}(\sum_{i=1}^{d} h_{2l, 2, i}),
\]

where \( h_{2l, 2, i} \) is the \( i \)-th copy of \( h_{2l, 2} \) whose defining monomial is \([2li + 1, 2li + 2, 2li + 3, 2li + 4]\). Now we can apply a direct sum decomposition (see Lemma 2) to the
above equation (2). We can divide the variables string by string so that

\[
\text{wt}(\sum_{i=1}^{d} h_{2i,2,i}) = \text{wt}(h_{2i,2,1})(2^{2n-2l} - \text{wt}(\sum_{i=1}^{d-1} h_{2i,2,i}))
\]

\[
+ (2^{2l} - \text{wt}(h_{2i,2,1}))\text{wt}(\sum_{i=1}^{d-1} h_{2i,2,i})
\]

Therefore we get the following result (see [7, Theorem 3]):

\[
(4) \quad \text{wt}(f_{2n,\chi}) = \text{wt}(\sum_{i=1}^{d} h_{2i,2,i}) = \frac{1}{2}(2^{2n} - (2^{2l} - 2\text{wt}(h_{2i,2}))^d)
\]

\[
\]"
the 2-function $f$. It follows from the basic theory of recursions (for example, [9, pp. 1-3]) that

$$W_{n,\chi} = \sum_{j=1}^{d(\chi)} c_{j,\chi} \alpha_{j,\chi}^n$$

for some complex numbers $c_{j,\chi}$.

We can now provide the recursion orders and recursion polynomials for the different $\chi$-values. We begin with the following definition.

**Definition 9.** Consider a fixed $\chi$. We define the crucial weights (resp. crucial (Walsh) values) for $\chi$ to be the sequence of weights $wt(f_{k,\chi})$, $k = 2, 3, \ldots$ (respectively, sequence of Walsh values $W_{k\chi/2,\chi}$, $k = 2, 3, \ldots$), where $f_{2n,\chi} = 2-(1, 2, \chi + 1, \chi + 2)_{2n}$.

By Lemma 3, all 2-functions with the same $\chi$-value are affine equivalent and since weight is affine invariant, we only need to consider the particular function $2-(1, 2, \chi + 1, \chi + 2)_{2n}$ in Definition 9.

**Lemma 5.** For even $\chi$-value, in order to determine the sequence of Walsh values $Wv(\chi) = \{W_{n,\chi} : n = 2, 3, \ldots\}$ (for the function $2-(1, 2, \chi + 1, \chi + 2)_{2n}$ and so for any 2-function with the same $\chi$-value), it suffices to know the sequence of crucial Walsh values $Cv(\chi) = \{W_{k\chi/2,\chi} : k = 2, 3, \ldots\}$ and the sequences $Wv(\chi')$ for all $\chi' < \chi$ such that $\chi'$ divides $\chi$. Thus all of the sequences $Wv(\chi)$, $\chi = 4, 6, 8, \ldots$ can be determined successively by finding $Wv(2)$ and then the successive sequences of crucial values $Cv(\chi)$, $\chi = 4, 6, \ldots$.

**Proof.** This follows from Lemma 3 and Definition 9.

The next lemma gives a recursion for the crucial weights (recall equation (6) which gives the relation between weights and Walsh values).

**Lemma 6.** For $\chi = 2q$, the crucial weights for $\chi$ satisfy the recursion of order $q+2$ whose polynomial is given by

$$G_{\chi}(x) = (x - 4q) \prod_{i=0}^{q} (x - (1 + \sqrt{7})^q - i(1 - \sqrt{7})^i)^1/q \zeta_j^q,$$

where $\zeta_q$ is a primitive $q$-th root of unity.

**Proof.** See the proof of [7, Lemma 8], we use $\sqrt{7}$ instead of $\sqrt{5}$ in this lemma.

We provide the recursion polynomials using Theorem 6. This is another method for finding recursion polynomials, and if $q = \chi/2$ then the order of the recursion for $mf2$ functions is $q^2 - q + 3$ (see Theorem 7 below).

The following theorem gives an explicit formula, including the roots, for the recursion polynomials $F_\chi(x)$ defined above.

**Theorem 7.** Let $\chi = 2q$. Then the sequence of weights $wt(f_{2n,\chi})$, $n = q+1, q+2, \ldots$ satisfies a recursion of order $q^2 - q + 3$ which has recursion polynomial

$$F_\chi(x) = (x - 4)(x^2 - 2x - 6) \prod_{i=1}^{q-1} \prod_{j=1}^{q} (x - ((1 + \sqrt{7})^q - i(1 - \sqrt{7})^i)^1/q \zeta_j^q),$$

where $\zeta_q$ is a primitive $q$-th root of unity.
Proof. We can use the proof of [7, Theorem 4], with $\sqrt{7}$ instead of $\sqrt{5}$ in that proof.

Example 3. Let $\chi = 8 = 2 \cdot 4$. In this case, $q = 4$, which has one nontrivial divisor $d = 2$. We have

\[
\mathrm{wt}(f_{2n,8}) = \frac{1}{2}(4^n - (1 + \sqrt{7})^n - (1 - \sqrt{7})^n)
\]
\[
- (1^n + (-1)^n)((1 + \sqrt{7})(1 - \sqrt{7})^{n/2})
\]
\[
- \frac{1}{4}(1^n + (-1)^n + i^n + (-i)^n)(2((1 + \sqrt{7})^3(1 - \sqrt{7}))^{n/4} +
\]
\[
3((1 + \sqrt{7})^2(1 - \sqrt{7})^2)^{n/4} + 2((1 + \sqrt{7})(1 - \sqrt{7})^3)^{n/4}) - E
\]

where E represents the repeated terms. Note that, when $n = 4k$, we have an extra copy of $((1 + \sqrt{7})^2(1 - \sqrt{7})^2)^k$ so we see $E = ((1 + \sqrt{7})^2(1 - \sqrt{7})^2)^k$. Thus

\[
\mathrm{wt}(f_{2n,8}) = \frac{1}{2}(4^n - (1 + \sqrt{7})^n - (1 - \sqrt{7})^n)
\]
\[
- (1^n + (-1)^n)((1 + \sqrt{7})^2(1 - \sqrt{7})^{n/4})
\]
\[
- \frac{1}{4}(1^n + (-1)^n + i^n + (-i)^n)(2((1 + \sqrt{7})^3(1 - \sqrt{7}))^{n/4} +
\]
\[
3((1 + \sqrt{7})^2(1 - \sqrt{7})^2)^{n/4} + 2((1 + \sqrt{7})(1 - \sqrt{7})^3)^{n/4})
\]

So the recursion polynomial for $\chi = 8$ is

\[
F_8 = (x - 4)(x^2 - 2x - 6) \prod_{k=1}^{3} \prod_{j=1}^{4} (x - ((1 + \sqrt{7})^{4-k})(1 - \sqrt{7})^{k/4})(i)^j
\]
\[
= x^{15} - 6x^{14} + 2x^{13} + 24x^{12} + 60x^{11} - 360x^{10} + 120x^9 + 1440x^8
\]
\[
- 2160x^7 + 12960x^6 - 4320x^5 - 51840x^4 - 46656x^3 + 279936x^2
\]
\[
- 93312x - 1119744
\]

This polynomial matches the results from Table 2 and $\deg(F_8) = 15 = 4^2 - 4 + 3 = q^2 - q + 3$, as required.

Corollary 6. If $\chi(1)$ divides $\chi(2)$, then $F_{\chi(1)}(x)$ divides $F_{\chi(2)}(x)$.

Proof. Suppose $\chi(1)$ divides $\chi(2)$, then there exists a positive integer $k$ such that $\chi(2) = k\chi(1)$. If we let $\chi(1) = 2q$, then we have $\chi(2) = k\chi(1) = 2qk$. So Theorem 7 implies the corollary.

We show $F_{\chi}(x)$ for $2 \leq \chi \leq 16$ in Table 2.

Lemma 7. Given any linear recursion of order $m$, any $2m + 1$ consecutive values of the recursion suffice to determine the recursion polynomial.
Lemma 9. If \( \text{wt}(f) = \text{wt}(g) \), then the recursion polynomial for \( f \) is
\[
\chi = \begin{pmatrix} F_\chi(x) \\
2 \quad (x - 4)(x^2 - 2x - 6) \\
4 \quad (x - 4)(x^2 - 2x - 6)(x^2 + 6) \\
6 \quad (x - 4)(x^2 - 2x - 6)(x^6 + 12x^3 - 216) \\
8 \quad (x - 4)(x^2 - 2x - 6)(x^2 + 6)(x^2 - 6)(x^8 + 96x^4 + 1296) \\
10 \quad (x - 4)(x^2 - 2x - 6)(x^{10} - 72x^5 - 7776)(x^{10} + 264x^3 - 7776) \\
12 \quad (x - 4)(x^2 - 2x - 6)(x^2 + 6)(x^4 - 6x^2 + 36)(x^6 - 12x^3 - 216) \\
14 \quad (x - 4)(x^2 - 2x - 6)(x^{14} - 1584x^7 - 2779936)(x^{14} + 432x^7 - 2779936) \\
16 \quad (x - 4)(x^2 - 2x - 6)(x^2 + 6)(x^2 - 6)(x^4 + 36)(x^8 - 96x^4 + 1296) \\
& \quad (x^8 + 96x^4 + 1296)(x^{16} + 3456x^8 + 1679616)(x^{16} + 14208x^8 + 1679616) \\
\end{pmatrix}
\]

Proof. This lemma is well known. The classic Berlekamp-Massey algorithm for actually computing the recursion polynomial from the given recursion values is given in [16].

Theorem 8. If \( f \) is any \( mf^2 \) quartic \( 2 \)-MRS function with \( \chi = \{ 2, 4 \} \), then the recursion polynomial for \( f \) is
\[
p(x) = x^5 - 6x^4 + 4x^3 + 12x^2 + 8x + 32 = (x - 4)(x^4 - 2x^3 - 4x^2 - 4x - 8)
\]

Proof. It suffices to compute the recursion for any \( f \) with the set of \( \chi \) values \( \{ 2, 4 \} \). One such function is \( 2-(1, 2, 3, 6)_{2n} \), and computation shows that the weights of this function for \( n = 4, 5, \ldots, 14 \) are \( 40, 216, 968, 4320, 18816, 80992, 344192, 1449856, 6061696, 25190400, 104152064 \). This is enough to determine the given recursion polynomial.

Theorem 9. Suppose \( \chi_f = p^{l+1}\{2, 4\} \) and \( \chi_g = p^{l+1}\{2, 4\} \), where \( p \) is prime, \( l = 0, 1, 2, 3, \ldots \). If \( n \equiv 0 \mod p^{l+1} \), then we have \( \text{wt}(f) = \text{wt}(g) \).

Proof. By Theorem 1, we may assume without loss of generality that \( f = (1, 2, 2p^l + 1, 2p^l + 2) \) and \( g = (1, 2, 2p^l+1, 1, 2p^l+1+2) \). Let \( h \) be any function with \( \chi_h = \{2, 4\} \).

Then by Corollary 1, if \( \gcd(n, p) = 1 \), then we have \( \text{wt}(h) = \text{wt}(f) \) and \( n < p^l \), and if \( \gcd(n, p) = 1 \), then we have \( \text{wt}(h) = \text{wt}(g) \) and \( n > p^l \).

So if \( n \equiv 0 \mod p \), then we have \( \text{wt}(f) = \text{wt}(g) \).

Example 4. \( \text{wt}(2-(1, 2, 7, 8)_{2n}) = \text{wt}(2-(1, 2, 19, 20)_{2n}) \), \( n \equiv 0 \mod 9 \)

Lemma 8. If \( f, g \) are \( mf^2 \) quartic \( 2 \)-MRS functions, \( n \) is odd and the \( \chi \) pairs for \( f, g \) are \( \{2, 4\}, \{4, 4\} \), then the recursion polynomial for \( f = g \) is
\[
p(x) = x^3 - 32x^2 + 292x - 576 = (x - 16)(x^2 - 16x + 36)
\]

Proof. This follows from Theorem 9, by using Corollary 1 and Table 2.

Lemma 9. If \( f, g \) are \( mf^2 \) quartic \( 2 \)-MRS functions, \( n \equiv 0 \mod 3 \) and the \( \chi \) pairs for \( f, g \) are \( \{2, 2\}, \{6, 6\} \), then the recursion polynomial for \( f = g \) is
\[
p(x) = x^6 - 108x^4 + 2600x^2 + 13824 = (x - 8)(x + 8)(x^4 - 44x^2 - 216)
\]

Proof. This follows from Theorem 9, by using Corollary 1 and Table 2.
4.2. The cases $\chi = \{\chi_1, \chi_2\}$ with $\chi_1 \neq \chi_2$. Here we shall use some results for short quartic MRS functions [5] to find the weight recursion polynomials. In particular, [5, Th. 1] shows that the weights of the short ordinary quartic MRS functions $(1, i, n + 1, n + i)_{2n}, n \geq 2i + 1$, for any fixed value of $i \geq 2$, can be found from the weights of the functions $2-(1, 2, \chi + 1, \chi + 2)_{2n}$, where $\chi$ is even and $i = (\chi/2) + 1$. The proof of [5, Th. 1] used Lemma 2.

We know that $\chi_1, \chi_2$ are even integers from Definition 7. Thus to find the weights we need only consider functions $2-(1, 2, \chi_1 + 1, \chi_2 + 2)_{2n}$, where $\chi_1, \chi_2$ are any even integers.

In this section we shall prove that we can find the weights of the short ordinary quartic MRS functions $(1, \frac{i+1}{2}, n+1, n+\frac{i+1}{2})_{2n}, n \geq 2i+1$, for any fixed value of some odd $i \geq 3$, provided we have the weights of the functions $2-(1, 2, \chi_1 + 1, \chi_2 + 2)_{2n}$, where $\chi = \{\chi_1, \chi_2\} = (i-1)\{a, b\}$, for some odd $i \geq 3$, and any positive integers $a, b$. We also show that the latter weights can be computed from the weights of the functions $2-(1, 2, 3, 8)_{2n}$ in case $a = 1, b = 3$, and $2-(1, 2, 5, 8)_{2n}$ in case $a = 2, b = 3$, etc. (Recall [4, Def. 1.1, p. 193] that a short quartic MRS function in $2n$ variables has only $n$ or possibly $n/2$ if $n$ is even) terms in its algebraic normal form, and all such functions have the form $(1, i, n + 1, n + i)_{2n}$ with $2 \leq i \leq \lfloor n/4 \rfloor + 1$.)

**Theorem 10.** For each fixed odd $i \geq 3$, the function $b_{n,i} = 2-(1, 2, i, 3i - 1)_{2n}, n \geq 2i + 1$ and $\chi = (i-1)\{1, 3\}$, is permutation equivalent to the short function $s_{n,i} = (1, \frac{i+1}{2}, n+1, n+\frac{i+1}{2})_{2n}$. If we define

$$\sigma_n(2j - 1) = j, 1 \leq j \leq n \text{ and } \sigma_n(2j) = n + \frac{j+2}{3}, 1 \leq j \leq n,$$

then $\sigma_n(b_{n,i}) = s_{n,i}$. □

**Proof.** Using (9), we verify $\sigma_n(b_{n,i}) = s_{n,i}$.

Note that the general method of [3] cannot be applied to the rotation symmetric functions $s_{n,i}$ since these functions have generating monomials which depend on $n$. To explain how to find the weights of the short quartic MRS functions, we shall use Lemma 2.

Next we need the weights for the functions $b_{n,3}$ for $n \geq 5$.

**Lemma 10.** Let $w_{n,3}$ denote $wt(b_{n,3}) = wt(2-(1, 2, 3, 8)_{2n})$ ($\chi = \{2, 6\}$) for $n \geq 5$. The sequence $\{w_{n,3} : n = 5, 6, \ldots\}$ satisfies a linear recursion with recursion polynomial

$$p(x) = (x - 4)(x + 2)(x^2 - 2)(x^5 - 4x^4 + 4x^3 - 8x^2 - 16).$$

We define $w_{n,3}$ for $1 \leq n \leq 4$ to be $1, 0, 16, 36$ respectively.

**Proof.** The method of [3] shows that the weights satisfy a linear recursion for $n \geq 4$. We easily find the recursion by computing $wt(b_{n,3})$ for $5 \leq n \leq 23$ (the values are 216, 888, 4320, 18544, 80512, 340320, 1437184, 6006720, 24990720, 103356288, 425773056, 1747287808, 7148904448, 29169876480, 118749724672, 482449652736, 1956639277056, 7923199899648, 32040871526400) and then using software (we used Mathematica command FindLinearRecurrence). The recursion can be extended backwards to give values for $w_{n,3}$ with $1 \leq n \leq 4$ (they are 1, 0, 16, 36), but these values do not equal any weights of $b_{n,3}$, which explains our condition $n \geq 5$ in the lemma. □
Let \( n \) be any \( m \ell^2 \) quartic 2-MRS function with \( \chi = \{4, 12\} \), then the recursion polynomial for \( b \) is

\[
(x - 4)(x + 2)(x^2 - 2)(x^2 + 2)(x^4 - 8)(x^5 - 4x^4 + 4x^3 - 8x^2 - 16)(x^{10} + 8x^8 + 16x^6 + 64x^4 + 512)(x^{20} - 16x^{16} - 192x^{12} - 1536x^8 - 4096x^4 - 8192)(x^{20} - 4x^{18} + 32x^{16} + 384x^{12} - 1536x^{10} - 3072x^8 + 12288x^6 - 16384x^4 - 32768x^2 + 65536).
\]

with degree 65.

Proof. We can get the result by Theorem 11 and then using software (we used Mathematica command FindLinearRecurrence).

Next we consider the case \( i = 7 \).

Theorem 13. Given \( n \geq 15 \), we have \( w_{n,7} = \text{wt}(b_{n,7}) = \text{wt}(2-(1, 2, 7, 20)_{2n}) \) for all \( n \not\equiv 0 \mod (3) \). If \( n \equiv 0 \mod (3) \) then

\[
\text{wt}(b_{n,7}) = \omega_{n/3,3}((2^{2n/3} - w_{2n/3,5}) + w_{2n/3,5}(2^{2n/3} - w_{n/3,5}).
\]

Proof. The first sentence of the theorem follows immediately from Corollary 2. If \( n \equiv 0 \mod (3) \), we apply Lemma 2 with \( k = 2n/3 \) to

\[
\sigma_n((2-(1, 2, 7, 20)_{2n}) = (1, 4, n + 1, n + 4)_{2n}
\]
by separating the variables according to the residues mod(3) of their indices. We define \( g_2 \) as a function of the \( k \) variables with indices \( \equiv 1 \) mod(3) and renumber those indices as \( 1,2,\ldots,k \), respectively. Thus (for \( n \geq 15 \)) \( g_2 = (1,2,(n/3)+1,(n/3)+2)_{2n/3} \) and \( wt(g_2) = wt(2-(1,2,3,8)_{2n/3}) = wt(b_{n/3}) = w_{n/3,3} \) since \( g_2 \) is the short function \( s_{n/3,3} \) and \( \sigma_{n/3}(b_{n/3}) = s_{n/3,3} \). For (12) we still get \( wt(g_2) = w_{n/3,3} \) by Lemma 10. We define \( h_2 \) in \( 2k \) variables as the direct sum of two functions, one in the \( k \) variables with indices \( \equiv 0 \) mod(3) and one in the \( k \) variables with indices \( \equiv 2 \) mod(3) By renumbering each of these two sets as before, both of these functions are equivalent to \( (1,2,(n/3)+1,(n/3)+2)_{2n/3} = g_2 \), so \( h_2 \) is equivalent to the direct sum \( g_2 \oplus g_2 \). Hence by the argument that gave (11) we have \( wt(h_2) = w_{2n/3,5} \). Now Lemma 2 gives (12).

\[ \square \]

**Example 6.** Let \( b_{15,7} = 2-(1,2,7,20)_{30} \). We take \( 2n = 30 \) so \( k = 10 \) in Lemma 2. Thus the 10 variables with indices 1,4,7,10,13,16,19,22,25,28 are renumbered as 1,2,3,4,5,6,7,8,9,10 and \( g_2 = (1,2,6,7)_{10} \), which is the short function \( s_{5,3} \). Thus \( h_2 \) in 20 variables is equivalent to \( s_{5,3} \oplus s_{5,3} \). Since \( \sigma_5(2-(1,2,3,8)_{10}) = (1,2,6,7)_{10} = s_{5,3} \), and \( wt(2-(1,2,3,8)_{10}) = 216 \), we have \( wt(h_2) = 2\cdot216 \cdot (2^{10} - 216) = 349,056 \). Now (12) gives \( wt(b_{15,7}) = 216(2^{20} - 349,056) + 349,056(2^{10} - 216) = 433,133,568 \).

Now we show the various cases, \( \chi = (i-1)\{1,4\} \) and \( \chi = (i-1)\{1,5\} \). Note that 3 of these already follow from Theorem 1 (Corollaries 3, 4 and 5 above).

**Theorem 14.** For each fixed odd \( i \geq 3 \), the function \( d_{n,i} = 2-(1,2,i,4i-2)_{2n} \), with \( n \geq 2i+1 \) and \( \chi = (i-1)\{1,4\} \), is permutation equivalent to the short function \( s_{n,i} = (1,\frac{i+1}{2},n+1,n+\frac{i+1}{2})_{2n} \). If we define

\[ \sigma_n(2j-1) = j, 1 \leq j \leq n \] and \( \sigma_n(2j) = n + \frac{j+3}{4}, 1 \leq j \leq n, \]
then \( \sigma_n(d_{n,i}) = s_{n,i} \).

**Proof.** Using (13), we verify \( \sigma_n(d_{n,i}) = s_{n,i} \).

**Theorem 15.** For each fixed odd \( i \geq 3 \), the function \( u_{n,i} = 2-(1,2,i,5i-3)_{2n} \), with \( n \geq 2i+1 \) and \( \chi = (i-1)\{1,5\} \), is permutation equivalent to the short function \( s_{n,i} = (1,\frac{i+1}{2},n+1,n+\frac{i+1}{2})_{2n} \). If we define

\[ \sigma_n(2j-1) = j, 1 \leq j \leq n \] and \( \sigma_n(2j) = n + \frac{j+4}{5}, 1 \leq j \leq n, \]
then \( \sigma_n(u_{n,i}) = s_{n,i} \).

**Proof.** Using (14), we verify \( \sigma_n(u_{n,i}) = s_{n,i} \).

Now we give the general case: \( \chi = (i-1)\{a,b\} \), where \( a,b \) are positive integers.

**Theorem 16.** For each fixed odd \( i \geq 3 \), the function \( y_{n,i} = 2-(1,2,a(i-1)+1,b(i-1)+2)_{2n} \), with \( n \geq 2i+1 \) and \( \chi = (i-1)\{a,b\} \), where \( a,b \) are positive integers, is permutation equivalent to the short function \( s_{n,i} = (1,\frac{i+1}{2},n+1,n+\frac{i+1}{2})_{2n} \). If we define

\[ \sigma_n(2j-1) = \frac{j+(a-1)}{a}, 1 \leq j \leq n \] and \( \sigma_n(2j) = n + \frac{j+(b-1)}{b}, 1 \leq j \leq n, \]
then \( \sigma_n(y_{n,i}) = s_{n,i} \).

**Proof.** Using (15), we verify \( \sigma_n(y_{n,i}) = s_{n,i} \).
Next we show the special case, $a = 2, b = 3$ in Theorem 16. We need the weights for the functions $y_{n,3}$ for $n \geq 5$.

**Lemma 11.** Let $W_{n,3}$ denote $wt(y_{n,3}) = wt(2\cdot(1,2,5,8)_{2n})$ ($\chi = \{4,6\}$) for $n \geq 5$. The sequence $\{W_{n,3} : n = 5,6,\ldots\}$ satisfies a linear recursion with recursion polynomial

$$p(x) = (x-4)(x^8 - 2x^7 - 4x^6 - 24x^3 - 16x^2 + 32x + 64).$$

We define $W_{n,3}$ for $1 \leq n \leq 4$ to be $1,2,16,40$ respectively.

**Proof.** The method of [3] shows that the weights satisfy a linear recursion for $n \geq 5$. We easily find the recursion by computing $wt(y_{n,3})$ for $5 \leq n \leq 23$ values are $196, 8964320, 15816, 80512, 340832, 1437184, 6016000, 25020672, 103485440, 426194176, 1748975616, 7155275776, 29194760192, 118843580416, 482805995520, 1957982158848, 7928272486400, 32059962212352$ and then using software (we used Mathematica command FindLinearRecurrence). The recursion can be extended backwards to give values for $W_{n,3}$ with $1 \leq n \leq 4$ (they are $1,2,16,40$), but these values do not equal any weights of $y_{n,3}$, which explains our condition $n \geq 5$ in the lemma.

Now we show that we can compute the values

$$(16) \quad W_{n,i} = wt(y_{n,i}) = wt(2\cdot(1,2,2i-1,3i-1)_{2n}), \quad \text{odd } i \geq 3 \text{ and } n \geq 2i+1$$

by using Theorem 14, Lemma 2 and suitable decompositions of the short functions $s_{n,i} = (1, \frac{i+1}{2}, n+1, n + \frac{i+1}{2})_{2n}$.

We begin with a detailed exposition of the case $i = 5$, followed by an example for the convenience of the reader.

**Theorem 17.** We have $W_{n,5} = wt(y_{n,5}) = wt(2\cdot(1,2,9,14)_{2n})$ ($\chi = \{8,12\}$) equal to $wt(y_{n,3})$ for all odd $n \geq 7$. If $n$ is even then

$$wt(y_{n,5}) = 2W_{n/2,3}(2^n - W_{n/2,3}) \text{ for } n \geq 7.$$ 

**Proof.** The first sentence of the theorem follows immediately from Corollary 5. For $n$ even, we have from Theorem 16 ($a = 2, b = 3, i = 5$) that

$$\sigma_{n/2}(2\cdot(1,2,9,14)_{2n}) = (1,3,n+1,n+3)_{2n} = s_{n,5},$$

which is a pure short function since $n$ is even. Since the even index variables do not appear in $s_{n,5}$, we can use Lemma 2 by renumbering the first $n$ odd indices with $1,2,\ldots,n$ in order and renumbering the final $n$ variables in the same way. This gives $v = 2n, k = n$ and $g_2 = h_2 = (1,2,(n/2)+1,(n/2)+2)_n = s_{n/2,3}$, so $s_{n,5}$ is the direct sum of two copies of $s_{n/2,3}$. By Theorem 14, $\sigma_{n/2}(2\cdot(1,2,5,8)_{n}) = s_{n/2,3}$, so Lemma 2 gives (17). Note that we need some values for $W_{n,3}$ with $n \leq 4$ as given in Lemma 11.

**Example 7.** We take $n = 10$ so $k = 10$ in Lemma 2. Thus the 10 variables with indices $1,3,5,\ldots,15,17,19$ are renumbered as $1,2,3,\ldots,9,10$ and $g_2 = (1,3,6,8)_{10}$, which is the short function $s_{5,3}$. Thus $g_2 = h_2 = (1,3,6,8)_{10} = s_{5,3}$, so $s_{10,5}$ is the direct sum of two copies of $s_{5,3}$. By Theorem 14, $\sigma_5(2\cdot(1,2,5,8)_{10}) = (1,2,6,7)_{10} = s_{5,3}$. Since $wt(2\cdot(1,2,5,8)_{10}) = 196$, Now (17) gives $wt(y_{10,5}) = 2 \cdot 196(2^{10} - 196) = 324576$. 
Corollary 7. If \( y \) is any \( mf^2 \) quartic 2-MRS function with \( \chi = \{8, 12\} \), then the recursion polynomial for \( y \) is
\[
p(x) = (x - 4)(x^8 - 2x^7 - 4x^6 - 16x^4 - 24x^3 - 16x^2 + 32x + 64)(x^{56} + 4x^{54} + 16x^{52} + 256x^{50} + 576x^{48} - 1152x^{46} - 33792x^{44} - 116736x^{42} + 110592x^{40} - 184320x^{38} + 2019328x^{36} + 507904x^{34} + 24444928x^{32} + 139460608x^{30} - 37748736x^{28} + 466616320x^{26} + 23086720x^{24} - 285212672x^{22} + 469762048x^{20} - 31406948352x^{18} + 8858370048x^{16} - 35433480192x^{14} - 219043332096x^{12} + 103079215104x^{10} + 481036337152x^6 + 274877906944x^4 + 1099511627776x^2 + 439804651104)
\]
with degree 65.

Next we consider the case \( i = 7 \).

Theorem 18. If \( n \geq 15 \), we have \( W_{n,7} = wt(y_{n,7}) = wt(2 \cdot (1, 2, 13, 20)_2n) \) (\( \chi = \{12, 18\} \)) equal to \( wt(y_{n,3}) \) for all \( n \not\equiv 0 \mod (3) \). If \( n \equiv 0 \mod (3) \) then
\[
wt(y_{n,7}) = W_{n/3,3}(2^{2n/3} - W_{2n/3,5}) + W_{2n,3}(2^{2n/3} - W_{n/3,3}).
\]

Proof. The first sentence of the theorem follows immediately from Corollary 5. If \( n \equiv 0 \mod (3) \), we apply Lemma 2 with \( k = 2n/3 \) to
\[
\sigma_n(2 \cdot (1, 2, 13, 20)_2n) = (1, 4, n + 1, n + 4)_2n
\]
by separating the variables according to the residues mod(3) of their indices. We define \( g_2 \) as a function of the \( k \) variables with indices \( \equiv 1 \mod (3) \) and renumber those indices as \( 1, 2, \ldots, k \), respectively. Thus (for \( n \geq 15 \)) \( g_2 = (1, 2, (n/3) + 1, (n/3) + 2)_2n/3 \) and \( wt(g_2) = wt((1, 2, 3, 8)_2n/3) = wt(y_{n,3}) = W_{n/3,3} \) since \( g_2 \) is the short function \( s_{n/3,3} \). We define \( h_2 \) in \( 2k \) variables as the direct sum of two functions, one in the \( k \) variables with indices \( \equiv 0 \mod (3) \) and one in the \( k \) variables with indices \( \equiv 2 \mod (3) \). By renumbering each of these two sets as before, both of these functions are equivalent to \( (1, 2, (n/3) + 1, (n/3) + 2)_2n/3 = g_2 \), so \( h_2 \) is equivalent to the direct sum \( g_2 \oplus g_2 \). Hence by the argument that gave (17) we have \( wt(h_2) = W_{2n,3}/5 \). Now Lemma 2 gives (18).

Example 8. We take \( 2n = 30 \) so \( k = 10 \) in Lemma 2. Thus the 10 variables with indices 1, 4, 7, 10, 13, 16, 19, 22, 25, 28 are renumbered 1, 2, \ldots, 9, 10 and \( g_2 = (1, 2, 6, 7)_10 \), which is the short function \( s_{5,3} \). Thus \( h_2 \) in 20 variables is equivalent to \( s_{5,3} \oplus s_{5,3} \). Since \( s_5 = \{2 \cdot (1, 2, 5, 8)_10 = (1, 2, 6, 7)_10 \) and \( wt(2 \cdot (1, 2, 5, 8)_10 = 196 \), we have \( wt(h_2) = 2 \cdot 196 \cdot (210 - 196) = 324, 576 \). Now (18) gives \( wt(y_{15,7}) = 324, 576(2^{20} - 324, 576) + 324, 576(2^{10} - 196) = 410, 652, 928 \).

REFERENCES

[1] C. Carlet, G. Gao and W. Liu, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions, J. Comb. Th. A, 127 (2014), 161–175.
[2] A. Chirvasitu and T. W. Cusick, Affine equivalence for quadratic rotation symmetric Boolean functions, Designs, Codes and Cryptography, 88 (2020), 1301–1329.
[3] T. W. Cusick, Weight recursions for any rotation symmetric Boolean functions, IEEE Trans. Inform. Th., 64 (2018), 2962–2968.
[4] T. W. Cusick and Y. Cheon, Affine equivalence of quartic homogeneous rotation symmetric Boolean functions, Inform. Sci., 259 (2014), 192–211.
[5] T. W. Cusick and Y. Cheon, Weights for short quartic Boolean functions, Inform. Sci., 547 (2021), 18–27.
[6] T. W. Cusick, Y. Cheon and K. Dougan, Theory of 2-rotation symmetric quartic Boolean functions, *Inform. Sci.*, **508** (2020), 358–379.

[7] T. W. Cusick and B. Johns, Theory of 2-rotation symmetric cubic Boolean functions, *Designs, Codes and Cryptography*, **76** (2015), 113–133.

[8] T. W. Cusick and D. Padgett, A recursive formula for weights of Boolean rotation symmetric functions, *Discrete Appl. Math.*, **160** (2012), 391–397.

[9] G. Everest, A. I. Shparlinski and T. Ward, *Recurrence Sequences*, Math. Surveys Monographs, 104, American Mathematical Society, Providence, 2003.

[10] S. Kavut and M. D. Yücel, Generalized rotation symmetric and dihedral symmetric Boolean functions - 9 variable Boolean functions with nonlinearity 242, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC 2007)*, Springer LNCS, 485, Springer, Berlin, 2007, 321–329.

[11] S. Kavut and M. D. Yücel, 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class, *Information and Computation*, **208** (2010), 341–350.

[12] S. Kavut, Results on rotation-symmetric S-boxes, *Information Sciences*, **201** (2012), 93–113.

[13] S. Kavut and S. Baloğlu, Classification of 6×6 S-boxes obtained by concatenation of RSSBs, in *Lightweight Cryptography for Security and Privacy*, Springer LNCS, 10098, Springer, Berlin, 2017, 110–127.

[14] S. Kavut and S. Baloğlu, Results on symmetric S-boxes constructed by concatenation of RSSBs, *Cryptogr. Commun.*, **11** (2019), 641–660.

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

[16] J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inform. Th.*, **15** (1969), 122–127.

Received October 2020; revised February 2021.

E-mail address: cusick@buffalo.edu
E-mail address: yhcrypt@gmail.com