Counting Equivalence Classes for Monomial Rotation Symmetric Boolean Functions with Prime Dimension

Thomas W. Cusick*, Pantelimon Stănică

Abstract

Recently much progress has been made on the old problem of determining the equivalence classes of Boolean functions under permutation of the variables. In this paper we prove an asymptotic formula for the number of equivalence classes under permutation for degree d monomial rotation symmetric (MRS) functions, in the cases where $d \geq 3$ is arbitrary and the number of variables n is a prime. Our counting formula has two main terms and an error term; this is the first instance of such a detailed result for Boolean function equivalence classes which is valid for arbitrary degree and infinitely many n. We also prove an exact formula for the count of the equivalence classes when $d = 5$; this extends previous work for $d = 3$ and 4.

Keywords: Boolean functions, rotation symmetric, affine equivalence, permutations, prime numbers.

1 Introduction

An n-variable Boolean function f is a map from the n dimensional vector space $\mathbb{F}_2^n = \{0,1\}^n$ into the two-element field $\mathbb{F}_2$, that is, a Boolean function can be thought of as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF)

$$f(x_1, \ldots, x_n) = a_0 + \sum_{1 \leq i \leq n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

*corresponding author, email: cusick@buffalo.edu

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$, and '+' is the addition operator over $\mathbb{F}_2$. The maximum number of variables in a monomial is called the (*algebraic*) *degree*. If all monomials in its ANF have the same degree, the Boolean function is said to be *homogeneous*. The integer n is the *dimension* of f.

Functions of degree at most one are called *affine* functions, and an affine function with constant term equal to zero is called a *linear* function. The *(Hamming) weight* $wt(\mathbf{x})$ (also called the binary sum of digits) of a binary string $\mathbf{x}$ is the number of ones in $\mathbf{x}$, and the *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is $wt(\mathbf{x}+\mathbf{y})$ (that is, the number of positions where $\mathbf{x}, \mathbf{y}$ differ). The nonlinearity of an n-variable function f is the minimum distance to the entire set of affine functions, which is known to be bounded from above by $2^{n-1} - 2^{n/2-1}$ (see [9] for more on cryptographic Boolean functions).

We define the (right) rotation operator ρ_n on a vector $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$ by $\rho_n(x_1, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1})$. Hence, ρ_n^k acts as a k-cyclic rotation on an n-bit vector. We extend it to monomials and binary strings, naturally. A Boolean function f is called *rotation symmetric* if for each input $(x_1, \ldots, x_n)$ in $\mathbb{F}_2^n$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n),$ for $1 \leq k \leq n$. That is, the rotation symmetric Boolean functions (RSBF) are invariant under cyclic rotation of inputs. Define $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) : 1 \leq k \leq n\}$, which generates a partition of cardinality g_n, and so, the number of n-variable RSBFs is 2^{g_n}. It was shown in [13] that $g_n = \frac{1}{n}\sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$, where ϕ is Euler's totient function. By abuse of notation, we also let $G_n(x_1 x_{i_2} \ldots x_{i_l}) = \{\rho_n^k(x_1 x_{i_2} \cdots x_{i_l}) : 1 \leq k \leq n\}$. We call a representation (not unique, since one can choose any representative in $G_n(x_1 x_{i_2} \ldots x_{i_l})$) of a rotation symmetric function $f(x_1, \ldots, x_n)$ the *short algebraic normal form* (SANF) if we write f as

$$a_0 + a_1 x_1 + \sum a_{1j} x_1 x_j + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where $a_0, a_1, a_{1j}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$, and the existence of a representative term $x_1 x_{i_2} \ldots x_{i_l}$ implies the existence of all the terms from $G_n(x_1 x_{i_2} \ldots x_{i_l})$ in the ANF. Note that x_1 always appears in the SANF of f. Certainly, the number of terms in the ANF of a monomial rotation symmetric function is a divisor of n (see [13]).

Throughout this paper we use the "capital mod" notation a Mod n to mean the unique integer $b \in \{1, 2, \ldots, n\}$ such that $b \equiv a \bmod n$.

If the SANF of f contains only one term, we call such a function a *monomial rotation symmetric* (MRS) function. In that case, the function f (of

degree d) has the form

$$f(\mathbf{x}) = x_1 x_{i_2} \dots x_{i_d} + x_2 x_{i_2+1} \dots x_{i_d+1} + ... + x_n x_{i_2-1} \dots x_{i_d-1}. \qquad (1)$$

Here and for the rest of the paper, the indices of the variables x_i are reduced Mod n.

If d divides n, then it is possible for some of the monomials in the representation (1) to be identical. If this happens, then we modify the definition of the function in (1) so that only the distinct monomials are used (the repeated monomials sum to zero). Such functions are called *short functions* (see [4, p. 5070] and [7, p. 193] for a description of the short functions for degrees 3 and 4, respectively). For the work in this paper, we do not need to pay any attention to the short functions.

We shall use the notation $(1, i_2, \dots, i_d)$ for the function $f(\mathbf{x})$ in (1), no matter how the terms on the right-hand side are written (so the order of the terms, and of the d variables in each term, does not matter). If $(1, i_2, \dots, i_d)$ is written in the form (1) (so the first subscripts in the n terms are $1, 2, \dots, n$ in order, and the other $d-1$ subscripts in order each give cyclic permutations of $1, 2, \dots, n$, as shown), we say f is written in *standard form*. Note that we do not require $i_j < i_{j+1}$, so there are $d!$ ways to write $f(\mathbf{x})$ in standard form. If we specify one representation of $f(\mathbf{x})$ (see the definition of $D_{d,n}$ below for a natural way to do this), then the standard form is unique. Ignoring the short functions, clearly each subscript j, $1 \le j \le n$, appears in exactly d of the terms in any representation of $f(\mathbf{x})$; we shall call these d terms the *j-terms* of f. We shall use the notation

$$[k_1, k_2, \dots, k_d] = x_{k_1} x_{k_2} \dots x_{k_d} \qquad (2)$$

as shorthand for the monomial on the right-hand side; note that the order of the variables matters, in particular the $d!$ permutations of $k_1, k_2, \dots, k_d$ give $d!$ different representations of form (2) for the same monomial $x_{k_1} x_{k_2} \dots x_{k_d}$.

Example 1.1. If $d = 3$, the cubic MRS function $(1, 2, 3)$ in 4 variables with $i_2 = 2,\ i_3 = 3$ in (1) can be written in standard form (not unique, and indeed this is an unusual standard form) as

$$x_3 x_2 x_1 + x_4 x_3 x_2 + x_1 x_4 x_3 + x_2 x_1 x_4.$$

There are 5 other standard forms, in which the variables in the first monomial $[3, 2, 1]$ above are permuted; the most natural of the 6 standard forms would begin with the monomial $[1, 2, 3]$. Note the 1-terms of this function are $[1, 2, 3], [1, 2, 4]$ and $[1, 3, 4]$.

We say that two Boolean functions $f(\mathbf{x})$ and $g(\mathbf{x})$ are *affine equivalent* if $g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b})$, where $A \in GL_n(\mathbb{F}_2)$ ($n \times n$ nonsingular matrices over the finite field $\mathbb{F}_2$ with the usual operations) and $\mathbf{b}$ is an n-vector over $\mathbb{F}_2$. We say $f(\mathbf{x}A + \mathbf{b})$ is a *nonsingular affine transformation* of $f(\mathbf{x})$. It is easy to see that if f and g are affine equivalent, then they have the same weight and nonlinearity. In general, these invariants are not sufficient, although we know that two quadratic functions are affine equivalent if and only if their weights and nonlinearities are the same–see [4, Lemma 2.3]. However, in general, that is not the case, for higher degrees.

In order to study the affine equivalence classes for the functions $(1, i_2, \ldots, i_d)$ we need to be able to identify all such functions which are distinct. We define

$$D_{d,n} = \{(1, i_2, \ldots, i_d) : \ 1 < i_2 < \ldots < i_d\},$$

where every such function is represented by the tuple with least i_2, and given that, with least i_3, ..., and given that with least i_d. Thus in $D_{d,n}$ each function is represented by a unique and natural standard form.

In [3] the authors introduced the notion of $\mathcal{P}$-*equivalence* $f \overset{\mathcal{P}}{\sim} g$, which is the affine equivalence of monomial rotation symmetric (MRS) functions f, g under permutation of variables (we will write here $f \sim g$, for easy displaying).

An $n \times n$ matrix C is *circulant*, denoted by $\mathrm{C}(c_1, c_2, \ldots, c_n)$, if all its rows are successive cyclic right rotations of the first row.

On the set $\mathcal{C}_n$ of circulant matrices an equivalence relation was introduced in [3]: for $A_1 = \mathrm{C}(a_1, \ldots, a_n)$, $A_2 = \mathrm{C}(b_1, \ldots, b_n)$, then $A_1 \approx A_2$ if and only if $(a_1, \ldots, a_n) = \rho_n^k(b_1, \ldots, b_n)$, for some $0 \leq k \leq n-1$. It was shown that the set of equivalence classes (with notation $\langle \cdot \rangle$) form a commutative monoid, under the natural operation $\langle A \rangle \cdot \langle B \rangle := \langle AB \rangle$. Define $\mathcal{C}_n^*$ to be the set of invertible $n \times n$ circulant matrices. Then the previous operation partitions these matrices into equivalence classes, say $\mathcal{C}_n^*/_{\approx}$, and consequently, $(\mathcal{C}_n^*/_{\approx}, \cdot)$ becomes a group.

Let $f = x_1 x_{j_2} \cdots x_{j_d} + x_2 x_{j_2+1} \cdots x_{j_d+1} + \cdots + x_n x_{j_2-1} \cdots x_{j_d-1}$ be an MRS function of degree d, with the SANF $x_1 x_{j_2} \cdots x_{j_d}$. We associate to f the (unique) equivalence class A_f of the circulant matrix $C(f) = \mathrm{C}(\overset{1}{\underset{\downarrow}{1}}, 0, \ldots, \overset{j_2}{\underset{\downarrow}{1}}, 0, \ldots, 0, \overset{j_3}{\underset{\downarrow}{1}}, \ldots, 0, \overset{j_d}{\underset{\downarrow}{1}}, \ldots, 0)$ whose first row has 1's in positions $\{1, j_2, \ldots, j_d\}$ given by the indices in the SANF monomial of f. We say that A_f is a *circulant matrix equivalence class*. Throughout this paper, we only consider circulant matrices whose entries are 0 and 1; we call these matrices 0/1-*circulants*.

For a binary (row) vector $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$, we let $\delta(a_1, a_2, \ldots, a_n) = \{i : a_i = 1\}$, and by abuse of notation, $\delta(C(\mathbf{a})) = \delta(\mathbf{a})$. We say that the vector $\mathbf{a}$ has *support* $\delta(\mathbf{a})$. Similarly, for a single monomial term $x_{i_1}x_{i_2}\cdots x_{i_d}$ of degree d in n variables, we define $\delta(x_{i_1}x_{i_2}\cdots x_{i_d}) = \{i_j : j = 1, 2, \ldots, d\}$. We can also extend the notion of support to the MRS function $f = x_{i_1}x_{i_2}\cdots x_{i_d}$ with this SANF, namely we define $\delta(f) = \delta(x_{i_1}x_{i_2}\cdots x_{i_d})$, which is not unique, but we prefer (so not to complicate the notation) to consider all such sets equal under a cyclic rotation permutation of the indices. That is, for A_f as above then $\delta(f) = \{1, j_2, \ldots, j_d\} = \{2, j_2 + 1, \ldots, j_d + 1\} = \cdots$.

We define the *(circulant) weight* of a 0/1-circulant to be the number of 1's in each row, that is, the size of the support of any row.

Example 1.2. Let $n = 3, d = 2$ and the MRS $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3x_1$ whose SANF is x_1x_2, say. Then the associated circulant matrix class is $A_f = \langle \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \rangle$ of weight 2 with $\delta(f) = \{1, 2\} = \{2, 3\} = \{1, 3\}$.

We now consider another type of equivalence between circulant matrices, that can be extended to the equivalence classes we have defined. Two circulant matrices A, B are called *P-Q equivalent*, if $PB = AQ$, where P, Q are permutation matrices. The notion of P-Q equivalence extends naturally from circulant matrices to equivalence classes, as any product of permutation matrices is also a permutation matrix, and any two representative matrices A_1, A_2 of an equivalence class $\langle A \rangle$ are related by a rotation of the row order. The next result showed that the $\mathcal{P}$-equivalence can be investigated in the realm of circulant matrices.

Theorem 1.1 (Canright–Chung–Stănică [3])**.** *Two MRS Boolean functions f, g in n variables are $\mathcal{P}$-equivalent if and only if their corresponding circulant matrix equivalence classes A_f and A_g are P-Q equivalent.*

The next result moves the P-Q equivalence into residue classes for some specific weights.

Theorem 1.2 (Th. 7.2 of Wiedemann–Zieve [14])**.** *Let A, B be two $n \times n$ 0/1-circulants of (circulant) weight at most 5 whose first rows have support $\delta(A)$, respectively, $\delta(B)$, where n is odd (if the weight $k \in \{4, 5\}$, the prime factors of n should be greater than $2k(k-1)$). Then the following are equivalent:*

(*i*) *There exist* $u, v \in \mathbb{Z}_n$ *such that* $\gcd(u, n) = 1$ *and* $\delta(A) = u\delta(B) + v$.

(*ii*) A, B *are* P-Q *equivalent.*

(*iii*) *There is an* $n \times n$ *permutation matrix* P *such that* $AA^T = PBB^TP^{-1}$.

(*iv*) *The matrices* AA^T, BB^T *are similar.*

Remark 1.1. The lower bound $2k(k-1)$ on the prime factors is sufficient to prove that (*i*) and (*iv*) are equivalent in the cases $k \in \{4, 5\}$ of Theorem 1.2 above (see [14, Th. 7.2]). Computations suggest that this sufficient condition is far from necessary.

The case of quartic MRS was dealt with in [7] for prime dimensions. The equivalence of (*i*) and (*ii*) above is called the bipartite Ádám problem (see [14, Section 9]), which turns out to be true for any weight, if the dimension is a prime number (see Theorem 2.1 below).

We remind the reader that we use the "capital mod" notation a Mod n to mean the unique integer $b \in \{1, 2, \ldots, n\}$ such that $b \equiv a \bmod n$.

The main result of this paper is an asymptotic formula for the number of equivalence classes under permutation of the variables for any degree d MRS functions in a prime number of variables. We also find the exact number of equivalence classes (and representatives of these classes) for quintic (degree 5) MRS (that is, their SANF is $f = x_1x_ix_jx_kx_s$ with $\delta(f) = \{1, i, j, k, s\}$) in prime dimensions; the cubic and quartic cases were done previously in [4, Section 4] and [7, Section 2], respectively.

2 An estimate for the number of equivalence classes for degree d MRS functions in prime p dimension

Let $E_{d,p}$ be the number of equivalence classes of degree d MRS functions in p variables, where p is a prime. Our goal is to obtain a good estimate for the count $E_{d,p}$ of these equivalence classes. We will need the higher degree versions of several results from [4], but only in the case where the number of variables is prime. The restriction to this case greatly simplifies the proofs. A key theorem that we use is the following one, which says that the bipartite Ádám conjecture (that is, the equivalence of (*i*) and (*ii*) in Theorem 1.2

above) is true if the size n of the matrices is a prime. This fact is mentioned without proof in [14, Section 9], where it is stated that a method of Babai [2] for a related conjecture can be extended to this case. We thank Michael Zieve for supplying us with the proof given below.

Theorem 2.1. *Let $p > d$ be a prime number and let A, B be two $p \times p$ 0/1-circulants with weight d whose first rows have support $\delta(A)$, respectively, $\delta(B)$. Then the following are equivalent:*

(*i*) *There exist $u, v \in \mathbb{Z}_n$ such that $\gcd(u, p) = 1$ and $\delta(A) = u\delta(B) + v$.*

(*ii*) *A, B are P-Q equivalent.*

Proof. We use the standard notation $\langle g \rangle$ for the cyclic subgroup generated by g in a given group G. We define the $p \times p$ "shift matrix" S by $S = C(0, 1, 0, \ldots, 0)$. In the proof, it is convenient to bear in mind the obvious fact that a $p \times p$ matrix is a circulant of weight k if and only if it is a sum of k distinct powers of S.

We shall prove that the P-Q equivalence classes of (ii) are identical to the affine equivalence classes of (i). We consider an arbitrary matrix B which is P-Q equivalent to a fixed $p \times p$ circulant matrix A, so we let P and Q be permutation matrices such that $B = P^{-1}AQ$ is circulant. We can rewrite this condition in terms of S as

$$(PS^{-1}P^{-1})A(QSQ^{-1}) \;=\; A, \tag{3}$$

since a matrix M is circulant if and only if it commutes with S.

Let G (clearly a group) be the set of pairs (P, Q) of permutation matrices (with group operation $(P, Q)(P', Q') = (PP', QQ')$) such that $P^{-1}AQ = A$. Since S commutes with the circulant matrix A, we have (S, S) in G. Similarly, given permutation matrices P and Q, $P^{-1}AQ$ is a circulant matrix if and only if g defined by

$$g = (PSP^{-1}, QSQ^{-1})$$

is an element of G. We can identify the group of all $p \times p$ permutation matrices with the symmetric group S_p, so the matrix S is the permutation $S(i) = i + 1 \text{ Mod } p$ in S_p. From now on in this proof we use the elements of S_p instead of the corresponding permutations. The subgroup $H = \langle S \rangle$ of order p in S_p is clearly identical with its centralizer, and its normalizer $N(H)$ has order $p(p-1)$. In fact $N(H)$ is the set of all invertible linear maps $\mu(i) = ai + b \text{ Mod } p$, $\gcd(a, p) = 1$.

We shall prove that $B = P^{-1}AQ$ is affine equivalent to A (that is, there exist two matrices, P', Q', which belong to $N(H)$ such that $B = P'^{-1}AQ'$) as follows: assume $\langle g \rangle$ and $\langle (S, S) \rangle$ are conjugate in G (this will be shown next, under the condition that p is prime), say via element h in G such that

$$hgh^{-1} = (S, S)^i \text{ with } \gcd(i, n) = 1.$$

If we let $h = (U, V)$, this gives

$$(UPSP^{-1}U^{-1}, VQSQ^{-1}V^{-1}) = (S^i, S^i),$$

so the elements $P' = UP$ and $Q' = VQ$ normalize $\langle S \rangle$ and hence belong to $N(H)$. But then we obtain

$$P'^{-1}AQ' = P^{-1}U^{-1}AVQ = P^{-1}AQ$$

(since (U, V) is in G) and hence (since P' and Q' are invertible linear maps) $P^{-1}AQ$ is affine equivalent to A, as desired.

Thus to complete the proof that (ii) implies (i) we need to show that $\langle g \rangle$ and $\langle (S, S) \rangle$ are conjugate in G, and here we use our hypothesis that p is prime. The support of the first row of A does not consist entirely of cosets of some subgroup of $\mathbb{Z}$ Mod p if and only if G intersects $\langle S \rangle \times \langle S \rangle$ in $\langle S, S \rangle$. For p prime, this means the support is neither empty nor all of $\mathbb{Z}$ Mod p, which is certainly true for our circulant matrix A. Now the Sylow p-subgroup of $S_p \times S_p$ has order p^2, and so is Abelian. Therefore G also has an Abelian Sylow p-subgroup. Since $\langle S, S \rangle$ is a subgroup of order p in G, it is contained in a Sylow p-subgroup of g. But the centralizer of $\langle S, S \rangle$ in $S_p \times S_p$ is $\langle S \rangle \times \langle S \rangle$, which by hypothesis intersects G in $\langle S, S \rangle$, so $\langle S, S \rangle$ is a Sylow p-subgroup of G. Thus $\langle g \rangle$ and $\langle S, S \rangle$ are conjugate in G. Note that this proof shows we can explicitly specify the element h which gives the conjugacy by $h = (P'P^{-1}, Q'Q^{-1})$, but we do not need this fact. □

The next theorem is the analog of [4, Theorem 3.5], generalized to higher degrees. Note that we removed the *gcd* condition in that theorem, since it is always true when the number of variables is a prime.

Theorem 2.2. *Suppose $f = (1, a_2, \ldots, a_d)$ in standard form and $g = (1, b_2, \ldots, b_d)$ are degree $d \geq 3$ monomial rotation symmetric functions with a prime number $p > d$ of variables. If $\mu(f) = g$ for some permutation μ (that is, μ acts on the indices of the p input variables of f, transforming f into g), then there exists a permutation σ such that $\sigma(f) = g$,*

$\sigma([1, a_2, \ldots, a_d]) = [1, c_2, \ldots, c_d]$ *and* $\sigma(1) = 1$, *where* $[1, c_2, \ldots, c_d]$ *is one of the* 1*-terms in* g. *Also,* σ *satisfies*

$$\sigma(i) = (i-1)(\sigma(2)-1)+1 \text{ Mod } p,\ 1 \le i \le p. \tag{4}$$

Proof. Let $C(f)$ and $C(g)$ be the $p \times p$ circulant matrices defined in Section 1. By Theorem 2.1, we have $u, v \in \mathbb{Z}_n$ such that $\gcd(u, p) = 1$ and

$$\delta(g) = \{1, b_2, \ldots, b_d\} = u\delta(f) + v = \{1, u(a_2-1)+1, \ldots, u(a_d-1)+1\} \tag{5}$$

(note that we have subtracted $u + v - 1$ from each term in $u\delta(f) + v$ for the last equality). Now if we define the permutation σ by (4) with $\sigma(2) = u + 1$, then (5) along with the fact that $\gcd(u, p) = 1$ implies (recall that σ acts on indices)

$$\begin{aligned}\sigma(\delta(f)) &= \{1, (a_2-1)(\sigma(2)-1)+1, \ldots, (a_d-1)(\sigma(2)-1)+1\} \\ &= \{1, (a_2-1)u+1, \ldots, (a_d-1)u+1\} = \delta(g),\end{aligned}$$

which proves the theorem. □

Define

$$\sigma_{\tau,n}(i) = \sigma_\tau(i) = (i-1)\tau + 1 \text{ Mod } n,\ 1 \le i \le n \tag{6}$$

(we shall omit n in the subscript if its value is clear from the context). Define a group G_n by

$$G_n = \{\sigma_{\tau,n} : \gcd(\tau, n) = 1,\ 0 \le \tau \le n-1\},$$

where the group operation is permutation multiplication. Clearly the group G_n is isomorphic to the group U_n of units of $\mathbb{Z}_n^*$ given by $U_n = \{k : \gcd(k, n) = 1\}$ with group operation multiplication mod n, since the bijection $\sigma_\tau \leftrightarrow \tau$ is a group isomorphism.

The next theorem is the analog of [4, Theorem 3.8], generalized to higher degrees.

Theorem 2.3. *For prime* $p > d$, *group* G_p *acts on the set*

$$C_{d,p} = \{\textit{degree } d \textit{ MRS functions } f(\boldsymbol{x}) \textit{ in } p \textit{ variables}\}$$

by the definition

$$\sigma_{\tau,p}(f(\boldsymbol{x})) = \sigma_{\tau,p}((1, a_2, \ldots, a_d)) \tag{7}$$

where $f(\boldsymbol{x})$ *has the unique standard form* $(1, a_2, \ldots, a_d)$ *given for that function in* $D_{d,p}$. *The orbits for this group action are exactly the equivalence classes for* $C_{d,p}$ *under permutations which preserve rotation symmetry.*

Proof. The proof is a straightforward generalization of the proof of [4, Theorem 3.8]. The quartic version of this proof is given in [7, Th. 1.9, p. 197]. □

In estimating $E_{d,p}$, we shall make use of the fact that we can get a formula for $E_{d,p}$ by using the well-known Burnside's Lemma applied to the group G_p acting on $C_{d,p}$, as described in Theorem 2.3. We need the notation

$$\mathrm{Fix}(\sigma) = \textit{set of functions in } C_{d,p} \textit{ fixed by } \sigma,$$

in order to state our lemma.

Lemma 2.1. *For the group action of G_p on $C_{d,p}$, we have*

$$E_{d,p} = \frac{1}{|G_p|} \sum_{\sigma \in G_p} |\mathrm{Fix}(\sigma)|.$$

Proof. This is a special case of Burnside's Lemma for counting orbits. By Theorem 2.3, the orbits in this special case are the affine equivalence classes. □

For our upper bound on $E_{d,p}$, we shall need the following two lemmas concerning the values of $|\mathrm{Fix}(\sigma)|$.

Lemma 2.2. *Given $n = p$ prime, for the group action of G_p on $C_{d,p}$, we have*

$$|\mathrm{Fix}(\sigma_{p-1})| \leq p^{\lceil (d-1)/2 \rceil}, \tag{8}$$

where σ_{p-1} is given by $\sigma_{\tau,n}$ of (6) with $\tau = p-1, n = p$. In fact, the exact value of $|\mathrm{Fix}(\sigma_{p-1})|$ is given by

$$|\mathrm{Fix}(\sigma_{p-1})| = \binom{(p-1)/2}{\lceil (d-1)/2 \rceil}. \tag{9}$$

Proof. It follows from (6) that

$$\sigma_{p-1}(i) = 2 - i \text{ Mod } p. \tag{10}$$

This implies that, given a function f in p variables, there is a representation $f = (1, i_2, \ldots, i_d)$ (where $2 \leq i_2 < i_3 < \ldots < i_d \leq p$) such that if σ_{p-1} fixes f (that is, it takes a representative into another representative, which is a translation of the first one) there must exist an a such that $1 \leq a \leq p-1$ and

$$\begin{aligned}\sigma(f) &= (1, 2 - i_2, 2 - i_3, \ldots, 2 - i_d) \text{ by (10)} \\ &= (1 + a, i_2 + a, i_3 + a, \ldots, i_d + a), \text{ since } \sigma \text{ fixes } f\end{aligned}$$

(order here is not important; in a d-tuple representation for a function f, we always assume that the d entries are taken Mod p). Without loss of generality, assume that $1 = i_2 + a$. Hence, since $2 \leq i_2 < i_3 < \ldots < i_d \leq p$, we have

$$1 < 2 - i_d < 2 - i_{d-1} < \ldots < 2 - i_2 \text{ Mod } p$$

and

$$1 = i_2 + a < i_3 + a < \ldots < i_d + a < 1 + a \text{ Mod } p.$$

Putting these two together, we get the series of equalities

$$1 = i_2 + a, 2 - i_d = i_3 + a, 2 - i_{d-1} = i_4 + a, \ldots, 2 - i_2 = 1 + a. \qquad (11)$$

Thus, by choosing the $i_1, i_2, \ldots, i_{\lceil (d-1)/2 \rceil}$ from among $1, 2, \ldots p$, we create a function that is fixed by σ_p (since these choices determine the remaining i_j's). This leaves us with no more than $p^{\lceil (d-1)/2 \rceil}$ possible functions that are fixed by σ_p, which proves (8).

The proof of (9) is contained in the proof of Lemma 2.3 below. □

Recall that a *cyclotomic coset* of τ (τ-cyclotomic coset) modulo p (it can be defined in more generality, but we will only need this particular case) containing i is the set

$$C_i = \{i \cdot \tau^j \pmod p \in \mathbb{Z}_p : j = 0, 1, \ldots\}.$$

(Since we work with indices in $\{1, 2, \ldots, n\}$, we replace 0 with n in these cyclotomic sets, that is, we replace the (mod n) classes by Mod n classes.) It is known [11, Chapter 3, pp. 112–118; Chapter 4, pp. 122–127] that the τ-cyclotomic cosets form a partition of $\mathbb{Z}_p$ (so, they are equal or disjoint). Moreover, the cardinality of a τ-cyclotomic coset C_i is the multiplicative order $\text{ord}_p(\tau)$ of $\tau \pmod p$ (under the assumption that p is prime), that is, $|C_i| = \text{ord}_p(\tau)$, where $\text{ord}_p(\tau)$ is the smallest integer with $\tau^{\text{ord}_p(\tau)} \equiv 1 \pmod p$. It is obvious (by Fermat's Little Theorem) that $\text{ord}_p(\tau)$ is a divisor of $p - 1$. The number of τ-cyclotomic cosets (including the trivial one containing 0) is

$$r := 1 + \frac{p - 1}{\text{ord}_p(\tau)}.$$

Lemma 2.3. *Given $n = p$ prime and $2 < d \leq \frac{p-1}{2}$, for the group action of G_p on $C_{d,p}$, we have*

$$|\mathrm{Fix}(\sigma_\tau)| \leq |\mathrm{Fix}(\sigma_{p-1})| \text{ for } 2 \leq \tau < p-1. \tag{12}$$

Proof. Let $f = (1, i_2, \ldots, i_d) \in \mathrm{Fix}(\sigma_\tau)$. Thus, for every $0 \leq k \leq p-1$, there exists t_k such that (all equations are Mod p)

$$\begin{aligned} \sigma_\tau\left((1, i_2, \ldots, i_d)\right) &= (1, (i_2-1)\tau+1, \ldots, (i_d-1)\tau+1), \\ \sigma_\tau\left((1+k, i_2+k, \ldots, i_d+k)\right) &= (k\tau+1, (k+i_2-1)\tau+1, \ldots, (k+i_d-1)\tau+1) \\ &= (1+t_k, i_2+t_k, \ldots, i_d+t_k). \end{aligned}$$

(Recall that the order is unimportant in our function notation - see the Introduction.) Therefore, for fixed k, there exists a permutation $\pi := \pi_k \in S_d$ (the group of permutations in d symbols) such that (we let $i_1 = 1$ and the equations are Mod p)

$$\begin{aligned} &(k + i_{\pi(j)} - 1)\tau + 1 = i_j + t_k, 1 \leq j \leq d, \text{ that is,} \\ &t_k - (k-1)\tau - 1 = \tau\, i_{\pi(j)} - i_j, \text{ for any } 1 \leq j \leq d. \end{aligned} \tag{13}$$

Now, summing (13) for all $1 \leq j \leq d$, and denoting $\Lambda := \sum_{j=1}^{d} i_j$, we get

$$\begin{aligned} &dt_k - (k-1)\tau d - d = \tau\Lambda - \Lambda = (\tau-1)\Lambda, \text{ and so,} \\ &t_k - (k-1)\tau - 1 = (\tau-1)\Lambda d^{-1} = (\tau\, i_{\pi(j)} - i_j) \text{ Mod } p, \end{aligned} \tag{14}$$

which is independent of k, since τ, Λ, d do not depend upon k.

We rewrite (14) as

$$\tau\left(\Lambda d^{-1} - i_{\pi(j)}\right) = (\Lambda d^{-1} - i_j) \text{ Mod } p,$$

and denoting $I := \{\Lambda d^{-1} - i_j : \ 1 \leq j \leq d\}$ (observe that $\pi(I) = I$ for any permutation $\pi \in S_d$), we infer that I is invariant under multiplication by τ (or any power of it, of course) and consequently, I is a union of cyclotomic cosets of τ modulo p. If τ happens to be a primitive root modulo p, that is $\mathrm{ord}_p(\tau) = p-1$ (it is well known [12, Thm. 2.9] that there are $\phi(p-1) \geq \frac{p}{e^\gamma \log\log p} + O\left(\frac{p}{(\log\log p)^2}\right)$ such values of τ, where $\gamma = 0.57721566\ldots$ is Euler's constant), then there are exactly 2 cyclotomic cosets, and I of cardinality $2 < d \leq \frac{p-1}{2}$ cannot be a union of cyclotomic cosets.

We next assume that τ is not a primitive root. Let an MRS $f \in \mathrm{Fix}(\sigma_\tau)$. Given our discussion above, the set I for given f is invariant under multiplication by τ Mod p, and so the cardinality of $\mathrm{Fix}(\sigma_\tau)$ is no larger than the cardinality of the set of d-element unions of τ-cyclotomic cosets

For the rest of the proof, it is convenient to have a unique representation for the functions that we discuss, so we shall always assume any function f is represented in the unique standard form that f has in the set $D_{d,p}$ (see the Introduction).

Thus, every function in $\mathrm{Fix}(\sigma_\tau)$ corresponds uniquely to a d-element union of τ-cyclotomic cosets (the correspondence may not be bijective). Further, observe that the number of ways of selecting (unordered) τ-cyclotomic cosets is larger (given τ Mod $p > 1$) when $\mathrm{ord}_p(\tau) = 2$, that is, $\tau = p - 1$ Mod p (since, if $\tau \neq \pm 1$ Mod p, then $\mathrm{ord}_p(\tau) > 2$, and we have fewer τ-cyclotomic cosets to choose from). Therefore, to show our result, it will be sufficient to show that when $\tau = p - 1$ Mod p, in reality, $|\mathrm{Fix}(\sigma_{p-1})|$ is exactly given by the count of the different d-element unions of $(p-1)$-cyclotomic cosets Mod p.

If $g = (1, s_2, \ldots, s_d) \in \mathrm{Fix}(\sigma_{p-1})$ then, for every $0 \leq k \leq p-1$, there exists T_k such that (all identities are Mod p)

$$\begin{aligned} \sigma_{p-1}\left((1, s_2, \ldots, s_d)\right) &= (1, 2 - s_2, \ldots, 2 - s_d), \\ \sigma_{p-1}\left((1 + k, s_2 + k, \ldots, s_d + k)\right) &= (1 - k, 2 - s_2 - k, \ldots, 2 - s_d - k) \\ &= (1 + T_k, s_2 + T_k, \ldots, s_d + T_k). \end{aligned}$$

(Again, the order is unimportant in the function notation.) Thus, for fixed k, there exists a permutation $\psi := \psi_k \in S_d$ such that $2 - s_j - k = s_{\psi(j)} + T_k$, for $1 \leq j \leq d$, or equivalently,

$$2 - k - T_k = (s_{\psi(j)} + s_j) \text{ Mod } p. \tag{15}$$

As for σ_τ, denoting $\Gamma := \sum_{j=1}^{d} s_j$, summing (15) for all j we obtain

$$2 - k - T_k = 2\Gamma d^{-1} = (s_{\psi(j)} + s_j) \text{ Mod } p, \tag{16}$$

independent of k. As before, it follows that the set $J := \{\Gamma d^{-1} - s_j : \ 1 \leq j \leq d\}$ (observe that $\psi(J) = J$ for any permutation $\psi \in S_d$) is invariant under multiplication by $(p-1)$ Mod p and so, J must be a d-element union of $(p-1)$-cyclotomic cosets. The (nontrivial) $(p-1)$-cyclotomic cosets are of the form $\{k, p-k\}$, $1 \leq k \leq (p-1)/2$. Therefore, if d is even, then $J = \{\{k_j, p - k_j\} : \ 1 \leq j \leq d/2\}$, where $1 \leq k_j \leq (p-1)/2$ and if d is odd we include the trivial coset in J.

We assume next that d is even (we will mention the differences, if any, for the case of d odd). To finish the proof, we need to show that any such d-element union generates a unique function in $\mathrm{Fix}(\sigma_{p-1})$, that is, the integers

s_j are uniquely determined by the k_j. Consider the system

$$\begin{cases} \Lambda\, d^{-1} - s_{2j-1} = k_j \\ \Lambda\, d^{-1} - s_{2j} = p - k_j \end{cases} \quad \text{for } 1 \le j \le d/2 \tag{17}$$

which implies that

$$s_{2j} - s_{2j-1} = 2k_j - p, 1 \le j \le d/2, \tag{18}$$

This implies that once s_{2j} is chosen, then s_{2j-1} is uniquely determined by (18). Therefore, the number of such choices for $\{s_{2j}\}$ is $\binom{(p-1)/2}{d/2}$ if d is even (if d odd, it would be $\binom{(p-1)/2}{(d-1)/2}$). This proves the lemma and also proves (9). (Observe that, given $g = (s_1, \ldots, s_d)$ in $\mathrm{Fix}(\sigma_{p-1})$, if we define k_j by (17) and (16), then $S = \{k_j, p - k_j\}$ is a union of $(p-1)$-cyclotomic cosets.) □

Next we need a result similar to Lemma 3.1 below. From now on, for brevity we use "MRS" to mean "MRS function(s)."

Lemma 2.4. *Let f be an MRS of degree d in prime p dimension whose support is $\delta(f) = \{1, i_2, \ldots, i_d\}$. Then, its equivalence class under permutation of variables contains an MRS g with support $\delta(g) = \{1, 2, j_3, \ldots, j_d\}$.*

Proof. We define the permutation $\sigma(i) = (i-1)(i_2-1)^{-1} + 1$ Mod p and we show that σ transforms f into another MRS g whose support contains $1, 2$. Certainly, $\sigma(1) = 1, \sigma(i_2) = 2$. We need to show that $g = \sigma \circ f$ is an MRS. This is achieved by induction observing that

$$\begin{aligned} \sigma((2, i_2+1, \ldots, i_d+1)) &= ((i_2-1)^{-1}+1, i_2(i_2-1)^{-1}+1, \ldots, i_d(i_2-1)^{-1}+1) \\ &= (i_2-1)^{-1} + (1, 2, \ldots, (i_d-1)(i_2-1)^{-1}+1) \\ &= (i_2-1)^{-1} + \sigma((1, i_2, \ldots, i_d)). \end{aligned}$$

Similarly, for every k (recall that indices are taken Mod p)

$$\sigma((1+k, i_2+k, \ldots, i_d+k)) = (i_2-1)^{-1} + \sigma((k-1, i_2+k-1, \ldots, i_d+k-1)),$$

and since p is prime (so the shift $(i_2-1)^{-1}$ is coprime to p), then adding $(i_2-1)^{-1}$ to the first output will cover all of the d-tuples, and so g is an MRS. □

By Lemma 2.4, we will find upper and lower bounds for the number of equivalence classes by looking at classes containing $\{1, 2, i_3, \ldots, i_d\}$ only.

Theorem 2.4. *The number of equivalence classes of degree $d \geq 3$ MRS functions in $p \geq 7$ (prime) variables satisfies*

$$\frac{1}{p(p-1)}\binom{p}{d} \leq E_{d,p} \leq \frac{1}{p(p-1)}\binom{p}{d} + \binom{(p-1)/2}{\lceil (d-1)/2 \rceil}. \tag{19}$$

Hence

$$E_{d,p} = \frac{1}{d!}p^{d-2} + O(p^{d-3}) \tag{20}$$

and also

$$E_{d,p} = \frac{1}{d!}\,p^{d-2} + \frac{1}{d!}\left(\frac{d^2-d-2}{2}\right)p^{d-3} + O(p^{d-4}) \text{ if } d \geq 5. \tag{21}$$

Proof. We give two proofs for the lower bound. First, we use necklace counting (see [13]) to find a formula for the number $|D_{d,n}|$ of MRS functions of degree d in n variables, namely

$$|D_{d,n}| = \frac{1}{n}\sum_{i|\gcd(n,d)} \phi(i)\binom{\frac{n}{i}}{\frac{d}{i}},$$

where ϕ is Euler's totient function. If we take $n = p$ prime, $p > d$, we get $|D_{d,p}| = \frac{1}{p}\binom{p}{d}$, and since the largest possible class has size $p-1$ we have the lower bound

$$E_{d,p} \geq \frac{1}{p(p-1)}\binom{p}{d} = \frac{1}{d!}p^{d-2} + O(p^{d-3}).$$

Second, two MRS f, g of (ordered) support $\delta(f) = \{1, 2, i_3, \ldots, i_d\}$ and $\delta(g) = \{1, 2, j_3, \ldots, j_d\}$ are equivalent if and only if the corresponding circulant matrices are P-Q equivalent if and only if (by Theorem 2.1) there exists $1 \leq u \leq p-1$ with $u\delta(f) + v = \delta(g)$. Certainly, for a fixed d-tuple $(1, 2, i_3, \ldots, i_d)$ there are $d!$ possible $(1, 2, j_3, \ldots, j_d)$, but since the first two indices are fixed, $(d-2)!$ of them are the same, that is, every fixed $(i_3, \ldots, i_d)$ will give rise to $\frac{d!}{(d-2)!} = d(d-1)$ putative $(j_3, \ldots, j_d)$. Thus, we obtain that the number of classes satisfies

$$E_{d,p} \geq \frac{1}{d(d-1)}\binom{p-2}{d-2} = \frac{1}{p(p-1)}\binom{p}{d},$$

so the lower bound by this method is the same as the bound above.

We now turn to the upper bound. Here we simply use Lemma 2.1. The $\mathrm{Fix}(\sigma_1)$ term in the sum is clearly

$$\frac{1}{p-1}|D_{d,p}| = \frac{1}{p(p-1)}\binom{p}{d} = \frac{1}{d!}\left(p^{d-2} - \left(\frac{d^2-d-2}{2}\right)p^{d-3}\right) + O(p^{d-4}) \tag{22}$$

for $d \geq 3$, and by Lemmas 2.2 and 2.3 the other $p-2$ terms in the sum each satisfy

$$\frac{1}{p-1}\mathrm{Fix}(\sigma) \leq \frac{1}{p-1}\binom{(p-1)/2}{\lceil (d-1)/2 \rceil} = O\left(p^{\lceil (d-3)/2 \rceil}\right). \tag{23}$$

Now (22) and (23) together give (20) and, for $d \geq 5$, also give (21). □

Remark 2.1. We observe that the lower bound of (19) is attained (assuming that the lower bound is replaced by the ceiling, of course). For example, if $p = 11, d = 3$, then $E_{d,p} = 2$, which equals the lower bound $\lceil 1.5 \rceil = 2$. In reality, the lower bound is always attained for primes $p \geq 7$ with $p \equiv 5 \pmod 6$, and degrees $d = 3$, since then the lower bound of (19) is $\lceil \frac{p-2}{6} \rceil = \lceil \frac{p}{6} \rceil = E_{3,p}$ (see [4]). From of the unimodality of the binomial coefficients, for p fixed, the smallest gap $(p-1)/2$ between the lower and upper bound is achieved when $d = 3$ (under the assumption that $3 \leq d \leq (p-1)/2$).

3 The exact number of quintic equivalence classes in prime dimension

We use the two Theorems 1.1 and 1.2 (or 2.1) to get an exact count for $E_{5,p}$, where p is a prime number. For easy displaying, we sometimes write $\frac{a}{b}$ to mean ab^{-1}, and $\sqrt{a}$ to mean $a^{1/2}$ (if it exists) in the prime field $\mathbb{F}_p$.

We start with a descriptive lemma detailing some representatives of the equivalence classes.

Lemma 3.1. *The $\mathcal{P}$-equivalence class of any quintic MRS h in n dimension, with $\delta(h) = \{1, i, j, k, s\}$ where at least one of* $\gcd(i-1,n), \gcd(j-1,n), \gcd(k-1,n), \gcd(s-1,n), \gcd(j-i,n), \gcd(k-i,n), \gcd(s-i,n), \gcd(k-j,n), \gcd(s-j,n), \gcd(s-k,n)$ *is 1 (which is always true for prime dimensions), contains a quintic MRS g with $\delta(g) = \{1, 2, a, b, c\}$.*

Proof. By Theorem 1.1 and Theorem 1.2 it will be sufficient to show that for every such MRS h with $\delta(h) = \{1, i, j, k, s\}$, there exists u, v such that $u\delta(h)+$

$v = \{1, 2, a, b, c\}$, for some a, b, c (we write $\{1, i, j, k, s\} \sim \{1, 2, a, b, c\}$). We assume that at least one of $\gcd(i-1, n) = 1$, $\gcd(j-1, n) = 1$, $\gcd(k-1, n) = 1$, $\gcd(i-j, n) = 1$, $\gcd(k-j, n) = 1$, $\gcd(k-i, n) = 1$ holds, say $\gcd(i-1, n) = 1$ (the other cases are similar). We easily see that taking $u = (i-1)^{-1}, v = 1-(i-1)^{-1}$, then $\{1, i, j, k, s\} \sim \{1, 2, a, b, c\}$ via u, v, where $a = 1+(j-1)(i-1)^{-1}$, $b = 1+(k-1)(i-1)^{-1}$, $a = 1+(s-1)(i-1)^{-1}$. $\square$

Since we have to consider several disjoint cases, we slightly change notations in this section. We denote by $E(p)_{k,\ell,\ldots}$ the number of distinct equivalence classes of quintic MRS in p variables, for $p \equiv k, \ell, \ldots \pmod{20}$, where $k, \ell, \ldots \in \{1, 3, 7, 9, 11, 13, 17, 19\}$.

Theorem 3.1. *Suppose $p \geq 7$ is a prime. Then the number of $\mathcal{P}$-equivalence classes of quintic MRS in p variables is*

$$E(p)_1 = \frac{p^3 - 9p^2 + 41p + 87}{120}, \qquad E(p)_{11} = \frac{p^3 - 9p^2 + 41p + 27}{120},$$
$$E(p)_{9,13,17} = \frac{p^3 - 9p^2 + 41p - 9}{120}, \qquad E(p)_{3,7,19} = \frac{p^3 - 9p^2 + 41p - 69}{120}.$$

Proof. Prime p must be at least 41 in order to use Lemma 3.1, since the proof of that lemma depends on Theorem 1.2. But we can verify Theorem 3.1 by calculation for $41 > p \geq 7$, so we can assume $p \geq 41$ in this proof. Since p is prime, by Lemma 3.1 it is sufficient to find the number of nonequivalent MRS with support $\{1, 2, a, b, c\}$. For that purpose, we fix $3 \leq j < k < s \leq p$ and look at possible $3 \leq a < b < c \leq p$ such that $\{1, 2, j, k, s\} \sim \{1, 2, a, b, c\}$. Solving the corresponding 120 systems and removing duplications we obtain the following 20 possible values of $\{a, b, c\}$ (unordered triples):

$$\begin{aligned}
&\{j, k, s\}\,; \{3-j, 3-k, 3-s\}\,; \\
&\left\{1+\frac{1}{j-1}, 1+\frac{k-1}{j-1}, 1+\frac{s-1}{j-1}\right\}; \left\{1+\frac{1}{k-1}, 1+\frac{j-1}{k-1}, 1+\frac{s-1}{k-1}\right\}; \\
&\left\{1+\frac{1}{s-1}, 1+\frac{j-1}{s-1}, 1+\frac{k-1}{s-1}\right\}; \left\{2-\frac{1}{j-1}, 2-\frac{k-1}{j-1}, 2-\frac{s-1}{j-1}\right\}; \\
&\left\{2-\frac{1}{k-1}, 2-\frac{j-1}{k-1}, 2-\frac{s-1}{k-1}\right\}; \left\{2-\frac{1}{s-1}, 2-\frac{j-1}{s-1}, 2-\frac{k-1}{s-1}\right\}; \\
&\left\{1-\frac{1}{j-2}, 1+\frac{k-2}{j-2}, 1+\frac{s-2}{j-2}\right\}; \left\{1-\frac{1}{k-2}, 1+\frac{j-2}{k-2}, 1+\frac{s-2}{k-2}\right\}; \\
&\left\{1-\frac{1}{s-2}, 1+\frac{j-2}{s-2}, 1+\frac{k-2}{s-2}\right\}; \left\{2+\frac{1}{j-2}, 2-\frac{k-2}{j-2}, 2-\frac{s-2}{j-2}\right\}; \\
&\left\{2+\frac{1}{k-2}, 2-\frac{j-2}{k-2}, 2-\frac{s-2}{k-2}\right\}; \left\{2+\frac{1}{s-2}, 2-\frac{j-2}{s-2}, 2-\frac{k-2}{s-2}\right\};
\end{aligned} \tag{24}$$

$$\left\{1-\frac{j-2}{k-j},1-\frac{j-1}{k-j},1+\frac{s-j}{k-j}\right\};\left\{1-\frac{j-2}{s-j},1-\frac{j-1}{s-j},1+\frac{k-j}{s-j}\right\};$$
$$\left\{1+\frac{k-1}{k-j},1+\frac{k-2}{k-j},1-\frac{s-k}{k-j}\right\};\left\{1+\frac{s-k}{s-j},1+\frac{s-2}{s-j},1+\frac{s-1}{s-j}\right\};$$
$$\left\{1-\frac{k-2}{s-k},1-\frac{k-1}{s-k},1-\frac{k-j}{s-k}\right\};\left\{1+\frac{s-j}{s-k},1+\frac{s-2}{s-k},1+\frac{s-1}{s-k}\right\}.$$

The set above would have a cardinality smaller than 20 if two (or more) such triples would overlap. Going diligently through the $\binom{20}{2}$ such systems (we used a Mathematica program to quickly sieve the output), we found the following possibilities when the set (24) shrinks.
Case 1. $j=3, s=4-k$ (we see below that this case includes $k=3-j, s=3\cdot 2^{-1}=\frac{p+3}{2}$; or, $k=j+1, s=1+j\cdot 2^{-1}=1+j\frac{p+1}{2}$; or, $k=2j-2, s=2j-1$, as well). The list of possible values for the triples $\{a,b,c\}$ in this case becomes

$$\begin{aligned}
&\{3,k,4-k\};\{0,3-k,k-1\};\\
&\left\{\frac{3}{2},\frac{5-k}{2},\frac{k+1}{2}\right\};\left\{\frac{2}{k-1},1+\frac{1}{k-1},1+\frac{2}{k-1}\right\};\\
&\left\{-\frac{2}{k-3},1-\frac{2}{k-3},1-\frac{1}{k-3}\right\};\left\{2-\frac{1}{k-1},2-\frac{2}{k-1},3-\frac{2}{k-1}\right\};\\
&\left\{2+\frac{1}{k-3},2+\frac{2}{k-3},3+\frac{2}{k-3}\right\};\left\{0,1+\frac{1}{k-2},1-\frac{1}{k-2}\right\};\\
&\left\{3,2-\frac{1}{k-2},2+\frac{1}{k-2}\right\};\left\{\frac{3}{2},\frac{1}{2}\left(3+\frac{1}{k-2}\right),\frac{1}{2}\left(3-\frac{1}{k-2}\right)\right\}.
\end{aligned}\tag{25}$$

If $p\equiv 1 \pmod 4$, by Gauss' reciprocity law, -1 is a quadratic residue modulo p, and so, for $\{k_0,4-k_0\}=\{2\pm(-1)^{1/2},2\mp(-1)^{1/2}\}$ Mod p (which happens when the first triple equals the eighth, that is, $k=2-(k-2)^{-1}$ Mod p, for example) the set (25) shrinks into the set of cardinality 5

$$\begin{aligned}
&\{3,k_0,4-k_0\};\{0,k_0-1,3-k_0\};\left\{\frac{2}{k_0-1},1+\frac{2}{k_0-1},1+\frac{1}{k_0-1}\right\};\\
&\left\{-\frac{2}{k_0-3},1-\frac{2}{k_0-3},1-\frac{1}{k_0-3}\right\};\left\{\frac{3}{2},\frac{1}{2}\left(3-\frac{1}{k_0-2}\right),\frac{1}{2}\left(3+\frac{1}{k_0-2}\right)\right\},
\end{aligned}$$

only one of which is of the form $\{3,k,s\}$. Otherwise, the set (25) has cardinality 10, only two of which have the form $\{3,k,s\}$. We note that here are $\frac{p-3}{2}$ ordered pairs $(k,4-k)$, with $k\geq 4$.

Case 2. $\{j,k,s\} = \left\{ \frac{5-\sqrt{5}-\sqrt{2\sqrt{5}-10}}{4}, \frac{7-\sqrt{5}-\sqrt{2\sqrt{5}-10}}{4}, \frac{12+\sqrt{10\sqrt{5}-50}-\sqrt{2\sqrt{5}-10}}{8} \right\}$ (and several like these, which are all included in the same class; we used the complex numbers representation to avoid cluttering). This is a slightly more complicated case to analyze.

It is well known (see [10, Theorem 97] that 5 is a quadratic residue for $p \equiv \pm 1 \pmod 5$ (which is the same as $p \equiv \pm 1 \pmod{10}$). Since this case does require it, we next assume that $p \equiv \pm 1 \pmod 5$. Next, we prove that if $p \equiv 1 \pmod 5$, then also $2\sqrt{5}-10$ is a quadratic residue modulo p, and so, all the above expressions for j,k,s exist modulo p. To show that, we take the minimal polynomial for $\sqrt{2\sqrt{5}-10}$, that is, $f(x) = x^4 + 20x^2 + 80$, which is seen to be irreducible by Eisenstein's criterion. The polynomial has discriminant $2^{16} \cdot 5^3$ (thus p does not divide the discriminant), its Galois group is the cyclic group of 4 elements (we also rechecked this by PARI/GP), and its roots in an extension of the prime field are $\alpha = \sqrt{2\sqrt{5}-10}, \beta = \sqrt{-2\sqrt{5}-10}, -\alpha, -\beta$ (the polynomial being biquadratic).

We may possibly use [1, Theorem 3.3] to show that if $p \equiv 1 \pmod 5$, then f splits completely over $\mathbb{Z}_p$, and if $p \equiv -1 \pmod 5$ it can be factored as a product of two irreducible polynomials of degree 2 (although, we do not need this second part), but one can also show this directly in the following way. The splitting field of f over the field of rational numbers $\mathbb{Q}$ is $\mathbb{Q}(\alpha,\beta)$. Since $\alpha\beta = -4\sqrt{5}$, then $\beta \in \mathbb{Q}(\alpha)$ and so, we have the tower of fields $\mathbb{Q} \overset{2}{\hookrightarrow} \mathbb{Q}(\sqrt{5}) \overset{2}{\hookrightarrow} \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$. Moreover, the splitting field of f, which we just showed is $\mathbb{Q}(\alpha)$, has degree 4 over $\mathbb{Q}$, which is the same as the degree of the cyclotomic extension of $\mathbb{Q}$ generated by $\zeta_5 = e^{2\pi i/5}$, which contains $\mathbb{Q}(\sqrt{5})$, since $2\sqrt{5}-10 = 2\sqrt{5}(1-\sqrt{5}) = -4(\zeta_5 + \overline{\zeta}_5)\left(1 + 2(\zeta_5 + \overline{\zeta}_5)\right)$. However, since $\zeta_5 = \frac{4\beta - \alpha\beta - 4}{16}$, then $\mathbb{Q}(\zeta_5) \hookrightarrow \mathbb{Q}(\alpha)$ and since they have the same degree over $\mathbb{Q}$, they must be equal.

Furthermore, the Frobenius automorphism takes ζ_5 to $\zeta_5^p = e^{2p\pi i/5}$, which fixes ζ_5 if $p \equiv 1 \pmod 5$, and moves it to $\overline{\zeta}_5$ (cycle of length 2) if $p \equiv -1 \pmod 5$. Thus, if $p \equiv 1 \pmod 5$, the above minimal polynomial splits into linear factors and if $p \equiv -1 \pmod 5$, it splits into quadratic factors.

Therefore, if $p \equiv 1 \pmod 5$, we have another equivalence class with representative $\{1,2,j,k,s\}$ of cardinality 4 (counting only the representatives $\{1,2,\ldots\}$).

Putting all these counts together, we find that the total contribution to

$E(p)_{(\cdot)}$ in the various cases is

$$E(p)_1 \leftarrow 1+1+\frac{\frac{p-3}{2}-1}{2}+\frac{\binom{p-2}{3}-5\cdot 1-4\cdot 1-10\cdot\frac{\frac{p-3}{2}-1}{2}}{20}=\frac{p^3-9p^2+41p+87}{120},$$

$$E(p)_{11} \leftarrow 1+\frac{\frac{p-3}{2}}{2}+\frac{\binom{p-2}{3}-4\cdot 1-10\cdot\frac{\frac{p-3}{2}}{2}}{20}=\frac{p^3-9p^2+41p+27}{120},$$

$$E(p)_{9,13,17} \leftarrow 1+\frac{\frac{p-3}{2}-1}{2}+\frac{\binom{p-2}{3}-5\cdot 1-10\cdot\frac{\frac{p-3}{2}-1}{2}}{20}=\frac{p^3-9p^2+41p-9}{120},$$

$$E(p)_{3,7,19} \leftarrow \frac{\frac{p-3}{2}}{2}+\frac{\binom{p-2}{3}-10\cdot\frac{\frac{p-3}{2}}{2}}{20}=\frac{p^3-9p^2+41p-69}{120},$$

and the theorem is shown. □

References

[1] W. W. Adams, Splitting of quartic polynomials, *Math. Comp.* **43:167** (1984), 329–343.

[2] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hung.* **29** (1977), 329–336.

[3] D. Canright, J.H. Chung, P. Stănică, Circulant Matrices and Affine Equivalence of Monomial Rotation Symmetric Boolean Functions, *Discrete Mathematics*, to appear.

[4] T. W. Cusick, Affine equivalence of cubic homogeneous rotation symmetric functions, *Inform. Sci.* **181:22** (2011), 5067–5083.

[5] T. W. Cusick, A. Brown, Affine equivalence for rotation symmetric Boolean functions with p^k variables, *Finite Fields Applic.* **18:3** (2012), 547–562.

[6] T. W. Cusick, Y. Cheon, Affine equivalence for rotation symmetric Boolean functions with 2^k variables, *Designs, Codes and Cryptography* **63** (2012), 273–294.

[7] T. W. Cusick, Y. Cheon, Affine equivalence of quartic homogeneous rotation symmetric Boolean functions, *Inform. Sci.* **259** (2014), 192–211.

[8] T. W. Cusick, P. Stănică, Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions, *Discrete Mathematics* **258** (2002), 289–301.

[9] T. W. Cusick, P. Stănică, Cryptographic Boolean functions and applications, Elsevier–Academic Press, 2009.

[10] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 1979.

[11] C. Huffman, V. Pless, Fundamentals of error–correcting codes, Cambridge University, 2004.

[12] H. L. Montgomery, R. C. Vaughan, Multiplicative Number Theory I: Classical Theory, Cambridge Studies in Adv. Math., 2012.

[13] P. Stănică, S. Maitra, Rotation Symmetric Boolean Functions – Count and Cryptographic Properties, *Discrete Appl. Math.* **156** (2008), 1567–1580.

[14] D. Wiedemann, M.E. Zieve, Equivalence of sparse circulants: the bipartite Ádám problem, manuscript; available at arXiv0706.1567v1 and www.math.lsa.umich.edu/∼zieve/papers/circulants.html.