2016-06-15

Counting permutation equivalent degree six binary polynomials invariant under the cyclic group

Luca, Florian; Stnic, Pantelimon

Springer

F. Luca, P. Stnic, "Counting permutation equivalent degree six binary polynomials invariant under the cyclic group," AAECC, v. 28 (2017), pp. 1-10
http://hdl.handle.net/10945/52632

AAECC (2017) 28:1–10
DOI 10.1007/s00200-016-0294-7

ORIGINAL PAPER

Counting permutation equivalent degree six binary polynomials invariant under the cyclic group

Florian Luca[1,4] · **Pantelimon Stănică**[2,3]

Received: 27 October 2015 / Revised: 20 May 2016 / Accepted: 2 June 2016 /
Published online: 15 June 2016

Abstract In this paper we find an exact formula for the number of affine equivalence classes under permutations for binary polynomials degree $d = 6$ invariant under the cyclic group (also, called monomial rotation symmetric), for a prime number of variables; this extends previous work for $2 \leq d \leq 5$.

Keywords Boolean functions · Rotation symmetric · Affine equivalence · Permutations · Prime numbers

Mathematics Subject Classification 94A60 · 94C10 · 06E30

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

✉ Pantelimon Stănică
pstanica@nps.edu

Florian Luca
florian.luca@wits.ac.za

1 School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, South Africa

2 Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943-5216, USA

3 Institute of Mathematics "Simion Stoilow" of the Romanian Academy, Bucharest, Romania

4 Centro de Ciencias Matematicas UNAM, Morelia, Mexico

as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF)

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

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*. A function of degree at most one is called *affine*; if it further has a constant term equal to zero is a *linear* function (see [8] for more on cryptographic Boolean functions).

We define the (right) rotation operator ρ_n on a vector $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ by $\rho_n(x_1, x_2, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1})$. Hence, ρ_n^k (the composition of ρ with itself k times) 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 it is invariant under cyclic rotation of inputs, that is, 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 $1 \le k \le n$. It is known [12] that the number of Boolean functions classes invariant under rotation symmetry is 2^{g_n}, where $g_n = \frac{1}{n} \sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$, and ϕ is Euler's totient function.

We call any representation 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 other in the rotation symmetry class.

If the SANF of f is of the form $x_1 x_{i_2} \ldots x_{i_d}$ (thus, its ANF is $f(\mathbf{x}) = x_1 x_{i_2} \ldots x_{i_d} + x_2 x_{i_2+1} \ldots x_{i_d+1} + \cdots + x_n x_{i_2-1} \ldots x_{i_d-1}$), we call such a function a *monomial rotation symmetric* (MRS) function (of degree d). We shall use the notation $(1, i_2, \ldots, i_d)$ for such a function, regardless of the order, among or within the terms. If d divides n, then it is possible for some of the monomials in the above representation to be identical, so the representation considers only one copy of each term. However, since we consider only prime dimensions, every term occurs only once.

We say that two Boolean functions $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ are *affine equivalent* if $g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b})$, for all $\mathbf{x} \in \mathbb{F}_2^n$, 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 nonlinearity are the same (see [4]). However, in general, that is not the case for higher degrees.

We say that two MRS f, g whose SANFs are $x_1 x_{i_2} \ldots x_{i_d}$, respectively, $x_1 x_{j_2} \ldots x_{j_d}$ are $\mathcal{P}$-*equivalent* [2] and written $f \overset{\mathcal{P}}{\sim} g$, if f, g are affine equivalent under a permutation of variables (we often write $f \sim g$, or, $x_1 x_{i_2} \ldots x_{i_d} \sim x_1 x_{j_2} \ldots x_{j_d}$, or even $(1, i_2, \ldots, i_d) \sim (1, j_2, \ldots, j_d)$, 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 (right) circular rotations of the first row. On the set $\mathcal{C}_n$ of circulant matrices an equivalence relation was introduced in [2]: 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 $\langle A \rangle \cdot \langle B \rangle := \langle AB \rangle$. Moreover, the previous operation partitions the invertible $n \times n$ circulant matrices into equivalence classes, say $\mathcal{C}_n^*/\!\approx$, and consequently, $(\mathcal{C}_n^*/\!\approx, \cdot)$ becomes a group.

Let f be an MRS function of degree d, with the SANF $x_1 x_{j_2} \ldots x_{j_d}$. We associate to f the (unique) equivalence class A_f of the circulant matrix $C(f)$ whose first row has 1's in positions $\{1, j_2, \ldots, j_d\}$ and 0's elsewhere. 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 $(a_1, a_2, \ldots, a_n)$ of dimension n, we let $\Delta(a_1, a_2, \ldots, a_n) \equiv \{i \,|\, a_i = 1\}$, 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 $x_{i_1} \ldots x_{i_d}$ of degree d in n variables, we define $\Delta(x_{i_1} \ldots x_{i_d}) \equiv \{i_j \,|\, j = 1, 2, \ldots, d\}$. We extend the notion of support to the MRS function f with SANF $x_{i_1} x_{i_2} \ldots x_{i_d}$ by $\Delta(f) = \Delta(x_{i_1} \ldots x_{i_d})$ (not unique, but we 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.

We recall now (see [2]) another type of equivalence between circulant matrices and their equivalence classes. 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 shows a connection between $\mathcal{P}$-equivalence and P–Q equivalence.

Theorem 1 (Canright–Chung–Stănică [2]) *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 fact (a case where the bipartite Ádám problem is true) is mentioned without proof in [13, Section 9], where it is stated that a method of Babai [1] for a related conjecture can be extended to this case. A proof (provided by the first author of [13]) can be found in Cusick and Stănică [9].

Theorem 2 *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 $u, v \in \mathbb{Z}_p$ such that* $\gcd(u, p) = 1$ *and* $\Delta(A) = u\Delta(B) + v$.
(ii) *A, B are P–Q equivalent.*

Cusick and Stănică [9] found the following asymptotic for the number of equivalence classes for any degree in prime dimension.

Theorem 3 (Cusick and Stănică [9]) *The number of equivalence classes of degree $d \geq 3$ MRS functions in $p \geq 7$ (prime) variables (where $p > d$) satisfies*

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

Hence,

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

and also

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

The main result of this paper is to find the *exact* number of equivalence classes (and representatives of these classes) for sextic (degree 6) MRS (whose SANF is $f = x_1x_ix_jx_kx_sx_t$ with $\Delta(f) = \{1, i, j, k, s, t\}$) in prime dimensions; the cubic, quartic and quintic cases were done previously in [2,4–7,9]; in [11], one of us completely solved the case of quartics in prime power dimension.

2 The result

Since the degree of our MRS will not change throughout, we let $E(p)$ be the number of equivalence classes of degree 6 MRS functions in p variables, where p is a prime number. We start with the following lemma, which enables us to narrow down the representatives of equivalence classes, whose proof (for any degree d) can be found in [9] (or, one can work it out easily using Theorem 2).

Lemma 4 *Let f be an MRS of degree 6 in prime p dimension whose support is $\Delta(f) = \{1, i_2, \ldots, i_6\}$. Then, its $\mathcal{P}$-equivalence class under permutation of variables contains an MRS g of support $\Delta(g) = \{1, 2, j_3, \ldots, j_6\}$.*

In this section, we use the Theorems 1 and 2 to get an exact count for $E(p)$, where p is a prime number. For easy writing, we sometimes write $\frac{a}{b}$ to mean ab^{-1}, or $\sqrt{a}$ to mean $a^{1/2}$, etc., in the prime field $\mathbb{F}_p$.

Since we have to consider several disjoint cases, we slightly change notations in this section. We denote by $E(p)_k$ the number of distinct equivalence classes under variable permutations of sextic MRS in p variables, for $p \equiv k \pmod{30}$, where $k \in \{1, 7, 11, 13, 17, 19, 23, 29\}$ (from past work, the count seemed to always depend upon residues modulo $(d-1)!$, although in this case, we compressed the count to residues modulo 30).

Theorem 5 *Suppose $p \geq 7$ is a prime. Then the number $E(p)_k$ of $\mathcal{P}$-equivalence classes of sextic MRS in p variables is*

$$E(p)_k = \begin{cases} \frac{p^4-14p^3+86p^2-194p+841}{720}, & k = 1 \\ \frac{p^4-14p^3+86p^2-194p+265}{720}, & k \in \{7, 13, 19\} \\ \frac{p^4-14p^3+86p^2-274p+921}{720}, & k = 11 \\ \frac{p^4-14p^3+86p^2-274p+345}{720}, & k \in \{17, 23, 29\}. \end{cases}$$

Proof Since p is prime, by Lemma 4 it is sufficient to find the number of nonequivalent MRS with support $\{1, 2, a, b, c, d\}$. For that purpose, we fix $3 \leq j < k < s < t \leq p$ and look at possible $3 \leq a < b < c < d \leq p$ such that $\{1, 2, j, k, s, t\} \sim \{1, 2, a, b, c, d\}$. By Theorem 2, two such tuples are equivalent if and only if there exist u, v such that $\{1, 2, j, k, s, t\} = u\{1, 2, a, b, c, d\} + v$. Given j, k, s, t, the values of a, b, c, d are determined by considering every possibility for $u(1, 2, a, b, c, d) + v$ among the 6! permutations of $\{1, 2, j, k, s, t\}$. While one can do it by hand (with enough patience), we used Mathematica to solve these 6! systems and removed duplications, and we obtained the following 30 possible values of $\{a, b, c, d\}$ (unordered tuples):

$\{j, k, s, t\}$; $\{3-j, 3-k, 3-s, 3-t\}$;

$$\left\{1+\frac{1}{j-1}, 1+\frac{k-1}{j-1}, 1+\frac{s-1}{j-1}, 1+\frac{t-1}{j-1}\right\}; \quad \left\{1+\frac{1}{k-1}, 1+\frac{j-1}{k-1}, 1+\frac{s-1}{k-1}, 1+\frac{t-1}{k-1}\right\};$$

$$\left\{1+\frac{1}{s-1}, 1+\frac{j-1}{s-1}, 1+\frac{k-1}{s-1}, 1+\frac{t-1}{s-1}\right\}; \quad \left\{1+\frac{1}{t-1}, 1+\frac{j-1}{t-1}, 1+\frac{k-1}{t-1}, 1+\frac{s-1}{t-1}\right\};$$

$$\left\{2-\frac{1}{j-1}, 2-\frac{k-1}{j-1}, 2-\frac{s-1}{j-1}, 2-\frac{t-1}{j-1}\right\}; \quad \left\{2-\frac{1}{k-1}, 2-\frac{j-1}{k-1}, 2-\frac{s-1}{k-1}, 2-\frac{t-1}{k-1}\right\};$$

$$\left\{2-\frac{1}{s-1}, 2-\frac{j-1}{s-1}, 2-\frac{k-1}{s-1}, 2-\frac{t-1}{s-1}\right\}; \quad \left\{2-\frac{1}{t-1}, 2-\frac{j-1}{t-1}, 2-\frac{k-1}{t-1}, 2-\frac{s-1}{t-1}\right\};$$

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

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

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

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

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

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

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

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

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

The set above would have a cardinality smaller than 30 if two (or more) such tuples would overlap. Using a Mathematica program to go through the $\binom{30}{2}=435$ such systems, we found the following *distinct* possibilities when the set (1) has fewer than 30 distinct elements.

Case 1. $j=2^{-1}(1-(-3)^{1/2}), k=j+2, s=2j, t=2j+1$ (or $j=2^{-1}(1+(-3)^{1/2}), k=j+2, s=2j, t=2j+1$, whose class is in fact equivalent to the previous one), under $p\equiv 1 \pmod 6$. Certainly, by Gauss' reciprocity, -3 is a quadratic residue modulo p if $p\equiv 1 \pmod 6$, and so, the above values exist. In this case the set (1) has cardinality 5

$$\{j,k,s,t\};\{3-j,3-k,3-s,3-t\};$$
$$\left\{1+\frac{1}{k-1},1+\frac{j-1}{k-1},1+\frac{s-1}{k-1},1+\frac{t-1}{k-1}\right\};$$
$$\left\{1+\frac{1}{s-1},1+\frac{j-1}{s-1},1+\frac{k-1}{s-1},1+\frac{t-1}{s-1}\right\};$$
$$\left\{1+\frac{1}{t-1},1+\frac{j-1}{t-1},1+\frac{k-1}{t-1},1+\frac{s-1}{t-1}\right\}.$$

The contribution to $E(p)_k$ is

$$1, \text{ if } k\in\{1,7,13,19\}.$$

Case 2. $\{j,k,s,t\}=\left\{\frac{2\sqrt{5}-3+\sqrt{2\sqrt{5}-5}}{\sqrt{5}-1},\frac{3\sqrt{5}+\sqrt{2\sqrt{5}-5}}{2\sqrt{5}},\frac{\sqrt{5}+\sqrt{2\sqrt{5}-5}}{\sqrt{5}-1},\frac{3-\sqrt{2\sqrt{5}-5}}{2}\right\}$ (there are other values, but they are all included in the same class; we used the complex numbers representation to avoid cumbersome notations). In this case the set (1) has cardinality 6.

The minimal polynomial of $\sqrt{2\sqrt{5}-5}$ is $f(x)=x^4+10x^2+5$, which is irreducible by Eisenstein's criterion, of discriminant $2^{12}\cdot 5^3$. The roots of the polynomial are $\alpha=\sqrt{2\sqrt{5}-5}$, $\beta=\sqrt{-2\sqrt{5}-5}$, $-\alpha,-\beta$. We showed (by a different method) in [9] that if $p\equiv 1 \pmod 5$, then $-10\pm 2\sqrt{5}$ are quadratic residues modulo p (regardless of the choice for the involved roots). We shall use this fact along with a result of Carlitz [3] (see also [10, Theorem 3]), who showed (among other things) that a polynomial of the form x^4+rx^2+s splits into the product of four distinct monic linear polynomials modulo p if and only if (throughout, $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol)

$$\left(\frac{s}{p}\right)=1,\left(\frac{r^2-4s}{p}\right)=1,\left(\frac{-r-2t}{p}\right)=1, \tag{2}$$

where $s \equiv t^2 \pmod{p}$. For our polynomial $x^4 + 10x^2 + 5$, taking $r = 10, s = 5$, then for $p \equiv 1 \pmod{5}$ (thus, $\left(\frac{5}{p}\right) = 1$), it is immediate that

$$\left(\frac{5}{p}\right) = 1, \left(\frac{10^2 - 4 \cdot 5}{p}\right) = \left(\frac{80}{p}\right) = \left(\frac{16 \cdot 5}{p}\right) = \left(\frac{5}{p}\right) = 1.$$

It suffices to show the last identity of (2) (for brevity, we use $t = \sqrt{5}$ for the integer t with $5 \equiv t^2 \pmod{p}$), that is

$$\left(\frac{-10 - 2\sqrt{5}}{p}\right) = 1,$$

i.e., $-10 - 2\sqrt{5}$ is a quadratic residue modulo p, which follows from our previous work [9], mentioned above.

Thus, if $p \equiv 1 \pmod{5}$, then we have another class of cardinality 6 whose representative can be taken to be $\{1, 2, j, k, s, t\}$ with $\{j, k, s, t\}$ given by the above values. The contribution to $E(p)_k$ is

$$1, \text{ if } k \in \{1, 11\}.$$

Case 3. $\{j, k, s, t\} = \left\{j, \frac{3-\sqrt{-3}}{2}, 1 + \frac{(2-j)(1-\sqrt{-3})}{2}, 2 + \frac{(1-j)(1+\sqrt{-3})}{2}\right\}$ (and the corresponding conjugate, all belonging to the same equivalence class). Certainly, these values exist if $p \equiv 1 \pmod{6}$, as we previously observed. In this case, the set (1) has cardinality 10. Counting all these tuples, we found $10(p-7)/6$ (since the degree of the function is 6 and there are $p - 7$ possible values for j, which renders 10 possible tuples; we also divided by 6, since order is not important, so for each value of j, say, there are 3! more tuples giving the same function). The number of classes in this case and the contribution to $E(p)_k$ is

$$\frac{p-7}{6}, \quad \text{if} \quad k \in \{1, 7, 13, 19\}.$$

Case 4. $\{j, k, s, t\} = \{j, 3 - j, s, 3 - s\}$ (or, $\{j, k, s, t\} = \{j, k, k + 1, k - j + 2\}$). This happens when $\{j, k, s, t\} = \{3 - k, 3 - j, 3 - t, 3 - s\}$ $\left(\text{respectively, } \{j, k, s, t\} = \left\{\frac{t-s}{k-s} + 1, \frac{s-2}{s-k} + 1, \frac{s-1}{s-k} + 1, \frac{j-s}{k-s} + 1\right\}\right)$. However, the two cases are equivalent, since any class with representative based on the first possibility contains a tuple based upon the second possibility. In this case the set (1) reduces to the following list of 15 possible values of $\{a, b, c, d\}$ (unordered tuples):

$$\{j, 3-j, s, 3-s\}; \quad \left\{\frac{1}{j-1}, \frac{j}{j-1}, \frac{j-s+1}{j-1}, \frac{j+s-2}{j-1}\right\};$$
$$\left\{1 + \frac{1}{2-j}, \frac{1}{2-j}, \frac{j-s-1}{j-2}, \frac{j+s-4}{j-2}\right\}; \quad \left\{\frac{1}{s-1}, \frac{s}{s-1}, \frac{-j+s+1}{s-1}, \frac{j+s-2}{s-1}\right\};$$
$$\left\{1 + \frac{1}{2-s}, \frac{1}{2-s}, \frac{-j+s-1}{s-2}, \frac{j+s-4}{s-2}\right\}; \quad \left\{2 + \frac{1}{1-j}, 3 + \frac{1}{1-j}, 2 + \frac{1-s}{j-1}, 2 + \frac{s-2}{j-1}\right\};$$

$$\left\{2+\frac{1}{1-s},3+\frac{1}{1-s},2+\frac{1-j}{s-1},2+\frac{j-2}{s-1}\right\};\quad \left\{2+\frac{1}{s-2},3+\frac{1}{s-2},2+\frac{2-j}{s-2},2+\frac{j-1}{s-2}\right\};$$
$$\left\{2+\frac{1}{j-2},3+\frac{1}{j-2},2+\frac{2-s}{j-2},2+\frac{s-1}{j-2}\right\};\quad \left\{\frac{2j-3}{j+s-3},\frac{2j+s-5}{j+s-3},\frac{2j+s-4}{j+s-3},\frac{3j+s-6}{j+s-3}\right\}$$
$$\left\{\frac{4-3j}{3-2j},\frac{5-3j}{3-2j},\frac{-3j+s+3}{3-2j},\frac{3j+s-6}{2j-3}\right\};\quad \left\{1+\frac{j-2}{j-s},1+\frac{j-1}{j-s},1+\frac{2j-3}{j-s},\frac{2j-3}{j-s}\right\};$$
$$\left\{\frac{j-3s+3}{j-s},\frac{3-2s}{j-s},1+\frac{s-2}{s-j},\frac{s-1}{s-j}+1\right\};\quad \left\{\frac{4-3s}{3-2s},\frac{5-3s}{3-2s},\frac{j-3s+3}{3-2s},\frac{j+3s-6}{2s-3}\right\};$$
$$\left\{\frac{2s-3}{j+s-3},\frac{j+2s-5}{j+s-3},\frac{j+2s-4}{j+s-3},\frac{j+3s-6}{j+s-3}\right\}. \tag{3}$$

For counting purposes, we consider only tuples $\{a,b,c,d\}$ in the list above satisfying $a+b\equiv 3 \pmod p, c+d\equiv 3 \pmod p$ (in some order), that is, we have the following tuples in list (3) satisfying these conditions

$$\{j,3-j,s,3-s\};$$
$$\left\{\frac{4-3j}{3-2j},\frac{5-3j}{3-2j},\frac{-3j+s+3}{3-2j},\frac{3j+s-6}{2j-3}\right\};$$
$$\left\{\frac{4-3s}{3-2s},\frac{5-3s}{3-2s},\frac{j-3s+3}{3-2s},\frac{j+3s-6}{2s-3}\right\}.$$

If $\{j,s\}=\left\{\frac{5\pm\sqrt{-3}}{4},\frac{7\pm\sqrt{-3}}{4}\right\}$ (which exists if $p\equiv 1 \pmod 6$) then there is only one possible value for $\{a,b,c,d\}$, namely

$$\{j,3-j,s,3-s\}.$$

The count for the number of tuples in this case is $\frac{(p-3)(p-5)}{8}$ (excluding the fixed tuple mentioned above) which gives a contribution to $E(p)_k$ of

$$\frac{1}{3}\left(\frac{(p-5)(p-3)}{8}-1\right)=\frac{(p-1)(p-7)}{24},\quad \text{if}\quad k\in\{1,7,13,19\},$$

and to $E(p)_k$ of

$$\frac{(p-3)(p-5)}{24},\quad \text{if}\quad k\in\{11,17,23,29\}.$$

In the remaining cases, every class will contain 30 elements, for a contribution to $E(p)_k$ of

$$\frac{\binom{p-2}{4}-5\cdot 1-6\cdot 1-10\cdot\frac{p-7}{6}-15\cdot\frac{(p-1)(p-7)}{24}}{30}=\frac{p^4-14p^3+56p^2-74p+31}{720},\quad \text{if}\quad k=1,$$
$$\frac{\binom{p-2}{4}-5\cdot 1-10\cdot\frac{p-7}{6}-15\cdot\frac{(p-1)(p-7)}{24}}{30}=\frac{p^4-14p^3+56p^2-74p+175}{720},\quad \text{if}\quad k\in\{7,13,19\},$$
$$\frac{\binom{p-2}{4}-6\cdot 1-15\cdot\frac{(p-3)(p-5)}{24}}{30}=\frac{p^4-14p^3+56p^2-34p-249}{720},\quad \text{if}\quad k=11,$$

$$\frac{\binom{p-2}{4} - 15 \cdot \frac{(p-3)(p-5)}{24}}{30} = \frac{p^4 - 14p^3 + 56p^2 - 34p - 105}{720} \quad \text{if} \quad k \in \{17, 23, 29\}.$$

Putting all these contributions together we find that

$$\begin{aligned}
E(p)_k &= 1 + 1 + \frac{p-7}{6} + \frac{(p-1)(p-7)}{24} + \frac{p^4 - 14p^3 + 56p^2 - 74p + 31}{720} \\
&= \frac{p^4 - 14p^3 + 86p^2 - 194p + 841}{720}, \quad \text{if} \quad k = 1, \\
E(p)_k &= 1 + \frac{p-7}{6} + \frac{(p-1)(p-7)}{24} + \frac{p^4 - 14p^3 + 56p^2 - 74p + 175}{720}, \\
&= \frac{p^4 - 14p^3 + 86p^2 - 194p + 265}{720}, \quad \text{if} \quad k \in \{7, 13, 19\}, \\
E(p)_k &= 1 + \frac{(p-3)(p-5)}{24} + \frac{p^4 - 14p^3 + 56p^2 - 34p - 249}{720} \\
&= \frac{p^4 - 14p^3 + 86p^2 - 274p + 921}{720}, \quad \text{if} \quad k = 11, \\
E(p)_k &= \frac{(p-3)(p-5)}{24} + \frac{p^4 - 14p^3 + 56p^2 - 34p - 105}{720} \\
&= \frac{p^4 - 14p^3 + 86p^2 - 274p + 345}{720}, \quad \text{if} \quad k \in \{17, 23, 29\},
\end{aligned}$$

which concludes the proof of the theorem. □

Acknowledgements We thank the anonymous referees for their very detailed and helpful comments. Work on this paper was partially done during an enjoyable visit of the second named author to the School of Mathematics of the Wits University in September 2015. We thank the School for Hospitality and excellent working conditions.

References

1. Babai, L.: Isomorphism problem for a class of point-symmetric structures. Acta Math. Acad. Sci. Hung. **29**, 329–336 (1977)
2. Canright, D., Chung, J.H., Stănică, P.: Circulant matrices and affine equivalence of monomial rotation symmetric Boolean functions. Discrete Math. J. **338**(12), 2197–2211 (2015)
3. Carlitz, L.: Note on a quartic congruence. Am. Math. Mon. **63**, 569–571 (1956)
4. Cusick, T.W.: Affine equivalence of cubic homogeneous rotation symmetric functions. Inform. Sci. **181**(22), 5067–5083 (2011)
5. Cusick, T.W., Brown, A.: Affine equivalence for rotation symmetric Boolean functions with p^k variables. Finite Fields Appl. **18**(3), 547–562 (2012)
6. Cusick, T.W., Cheon, Y.: Affine equivalence for rotation symmetric Boolean functions with 2^k variables. Des. Codes Crypt. **63**, 273–294 (2012)
7. Cusick, T.W., Cheon, Y.: Affine equivalence of quartic homogeneous rotation symmetric Boolean functions. Inform. Sci. **259**, 192–211 (2014)
8. Cusick, T.W., Stănică, P.: Cryptographic Boolean Functions and Applications. Elsevier, Amsterdam (2009)
9. Cusick, T.W., Stănică, P.: Counting equivalence classes for monomial rotation symmetric boolean functions with prime dimension. Cryptogr. Commun. (Discrete Struct. Boolean Funct. Seq.) **1**, 67–81 (2016)
10. Driver, E., Leonard, P.A., Williams, K.S.: Irreducible quartic polynomials with factorizations modulo p. Am. Math. Mon. **112**(10), 876–890 (2005)
11. Stănică, P.: Affine equivalence of quartic monomial rotation symmetric Boolean functions in prime power dimension. Inf. Sci. **314**, 212–224 (2015)

12. Stănică, P., Maitra, S.: Rotation symmetric Boolean functions—count and cryptographic properties. Discrete Appl. Math. **156**, 1567–1580 (2008)
13. Wiedemann, D., Zieve, M.E.: Equivalence of sparse circulants: the bipartite Ádám problem. Manuscript. arXiv:0706.1567v1. www.math.lsa.umich.edu/~zieve/papers/circulants.html