Turkish Journal of Mathematics

Volume 43 | Number 3 Article 25

1-1-2019

Value sets of folding polynomials over finite fields

ÖMER KÜÇÜKSAKALLI

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2019) 43: 1407 – 1413

doi:10.3906/mat-1812-64

Value sets of folding polynomials over finite fields

Ömer KÜÇÜKSAKALLI*
Department of Mathematics, Faculty of Arts and Science, Middle East Technical University, Ankara, Turkey

Received: 19.12.2018 • **Accepted/Published Online:** 26.03.2019 • **Final Version:** 29.05.2019

Abstract: Let k be a positive integer that is relatively prime to the order of the Weyl group of a semisimple complex Lie algebra $\mathfrak{g}$. We find the cardinality of the value sets of the folding polynomials $P_{\mathfrak{g}}^k(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}]$ of arbitrary rank $n \geq 1$, over finite fields. We achieve this by using a characterization of their fixed points in terms of exponential sums.

Key words: Lie algebra, Weyl group, fixed point, orbit, stabilizer

1. Introduction

Let p be a prime number and let $\mathbf{F}_q$ be a finite field of characteristic p. Given a polynomial $f(\mathbf{x}) \in \mathbf{Z}[x_1, \ldots, x_n]$, we consider the induced map $f : \mathbf{F}_q^n \to \mathbf{F}_q^n$. The problem of finding the cardinality of the value set $f(\mathbf{F}_q^n) = \{f(\mathbf{x}) : \mathbf{x} \in \mathbf{F}_q^n\}$ has been studied in various forms over the years. However, exact formulations for the cardinality are known only for polynomials in very specific forms. The results that apply to general polynomials are asymptotic in nature, or provide only estimates. We refer to the work of Mullen et al. [7] for an introduction of this problem, including several references and historical remarks. In this state of art, new families of polynomials for which we can find the cardinality of the value sets are of great interest.

A folding polynomial is a natural generalization of the Chebyshev polynomial [9]. There is only one semisimple complex Lie algebra of rank one, namely A_1, and the corresponding folding polynomials $P_{A_1}^k$ are the Chebyshev polynomials. The value sets of Chebyshev polynomials are first computed by Chou et al. [2]. There are three semisimple complex Lie algebras of rank two, namely A_2, B_2, and G_2. We have found the cardinality of the value sets of the folding polynomials $P_{A_2}^k$ in [4] and extended the idea for the polynomials $P_{B_2}^k$ and $P_{G_2}^k$ in [5]. However, this idea does not use the underlying algebraic structure in its full power and is complicated to be extended to higher ranks $n \geq 3$.

The folding polynomials $P_{\mathfrak{g}}^k$ are associated with semisimple complex Lie algebras and we need some notation to describe these polynomials. Let $\mathfrak{g}$ be a semisimple complex Lie algebra of rank n and $\mathfrak{h}$ its Cartan subalgebra, $\mathfrak{h}^*$ its dual space, $\mathcal{L}$ a lattice of weights in $\mathfrak{h}^*$ generated by the fundamental weights $\omega_1, \ldots, \omega_n$, and L the dual lattice in $\mathfrak{h}$. We define $\Phi_{\mathfrak{g}} : \mathfrak{h}/L \to \mathcal{C}^n$, induced from the action of W on $\mathcal{L}$, where $\Phi_{\mathfrak{g}} = (\varphi_1, \ldots, \varphi_n)$

$$\varphi_j(\mathbf{x}) = \sum_{w \in W} e^{2\pi i w(\omega_j)(\mathbf{x})}.$$

*Correspondence: komer@metu.edu.tr
2010 *AMS Mathematics Subject Classification:* 11T06

A theorem of Chevalley [1] leads to the following result which was first given by Veselov, and somewhat later by Hofmann and Withers independently.

Theorem 1.1 ([3, 8]) *With each semisimple complex Lie algebra $\mathfrak{g}$ of rank n, there is associated an infinite sequence of integrable polynomial mappings $P_{\mathfrak{g}}^k$, $k \in \mathbf{N}$ determined from the conditions*

$$\Phi_{\mathfrak{g}}(k\mathbf{x}) = P_{\mathfrak{g}}^k(\Phi_{\mathfrak{g}}(\mathbf{x})).$$

All coefficients of the polynomials defining $P_{\mathfrak{g}}^k$ are integers.

For a semisimple complex Lie algebra $\mathfrak{g}$ of rank n with roots λ_i, $i = 1, \ldots, n$, we identify $\mathfrak{h} = \oplus \mathcal{C}\lambda_i$ (respectively the lattice $L = \oplus \mathbf{Z}\lambda_i$) with $\mathcal{C}^n$ (respectively $\mathbf{Z}^n$). For $w \in W$, T_w is the $n \times n$ matrix representing the endomorphism $T_w : L \to L$ defined by $T_w(\lambda_i) = w(\lambda_i)$ for each $i = 1, \ldots, n$.

Note that T_w has integer coefficients and $\det(T_w) = \pm 1$. Let q be a power of a prime. Let I_n be the identity matrix of dimensions $n \times n$. An eigenvalue of the matrix T_w must be a root of unity. As a result, the matrix $qI_n - T_w$ is invertible (over rational numbers) since $q \geq 2$ is not a root of unity. The matrix $qI_n - T_w$ and its inverse are the main tools to study the polynomial mappings $P_{\mathfrak{g}}^k$.

Theorem 1.2 ([6]) *Let $\mathfrak{g}$ be a semisimple complex Lie algebra of rank n and let W be its Weyl group. Suppose that $p > n$. The polynomial mapping $P_{\mathfrak{g}}^k : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is a permutation if and only if $qI_n - T_w$ is invertible modulo k for each $w \in W$.*

The main idea of the proof of this theorem is to parametrize the elements of $\mathbf{F}_q^n$ by certain rational n-tuples. We summarize the consequences of this theorem, with some additional details that will be used in the current manuscript, as follows.

Let e be the exponent of the Weyl group and let ζ be a primitive root of unity of order $p^e - 1$. Let $\mathfrak{p}$ be a prime ideal $\mathfrak{p}$ of the cyclotomic extension $\mathbf{Q}(\zeta)$ lying over p. There is a one-to-one correspondence

$$\mathrm{Fix}(P_{\mathfrak{g}}^q) \longleftrightarrow \mathbf{F}_q^n$$

obtained by reducing the elements in $\mathrm{Fix}(P_{\mathfrak{g}}^q)$ modulo $\mathfrak{p}$. This correspondence is compatible under the action of $P_{\mathfrak{g}}^k$ on both sets. Given a matrix M with rational entries, we denote the free abelian group generated by its columns by $\mathrm{Col}(M)$. Consider $\mathrm{Col}\left((qI_n - T_w)^{-1}\right)$ which is a subgroup of $\mathbf{Q}^n$. This free subgroup is of rank n since the matrix $qI_n - T_w$ is invertible. Moreover it contains $\mathbf{Z}^n$. We define

$$X(w) := \mathrm{Col}\left((qI_n - T_w)^{-1}\right)/\mathbf{Z}^n$$

as a subgroup of $\mathbf{Q}^n/\mathbf{Z}^n$. We set

$$\mathcal{X} = \bigcup_{w \in W} X(w).$$

One can show that the set $\mathcal{X}$ is never a group. However, it is closed under the multiplication by integers. The set $\mathcal{X}$ parametrizes all the elements in $\mathrm{Fix}(P_{\mathfrak{g}}^q)$, and therefore all the elements in $\mathbf{F}_q^n$, with an n-tuple from $\mathbf{Q}^n/\mathbf{Z}^n$. More precisely, we have a surjective function

$$\Phi_{\mathfrak{g}} : \mathcal{X} \to \mathrm{Fix}(P_{\mathfrak{g}}^q).$$

Unfortunately, this map is not one-to-one. We define an equivalence relation on $\mathcal{X}$ to overcome this problem. For all $\mathbf{x},\mathbf{y}\in\mathcal{X}$, we set $\mathbf{x}\sim\mathbf{y}\iff\Phi_{\mathfrak{g}}(\mathbf{x})=\Phi_{\mathfrak{g}}(\mathbf{y})$. This definition allows us to extend the original one-to-one correspondence as follows:

$$\mathcal{X}/\sim\longleftrightarrow \mathrm{Fix}(P_{\mathfrak{g}}^{q})\longleftrightarrow \mathbf{F}_q^n.$$

After this brief summary of [6], we are now ready to study the value set $P_{\mathfrak{g}}^{k}(\mathbf{F}_q^n)$ by using $(k\mathcal{X})/\sim$.

2. Main results

The quotient set $(kX)/\sim$ and its order is closely related with the structures of the finite abelian groups $X(w)$. We claim that

$$X(w)\cong\mathbf{Z}^n/\mathrm{Col}(qI_n-T_w).$$

To justify this, we denote the columns of qI_n-T_w by $\mathbf{y}_i^w=(y_{1i},\ldots,y_{ni})$. Using the elementary column vectors $\mathbf{e}_1=(1,0,\ldots,0),\ldots,\mathbf{e}_n=(0,\ldots,0,1)$, we can write $\mathbf{y}_i^w=y_{1i}\mathbf{e}_1+\ldots+y_{ni}\mathbf{e}_n$. On the other hand, using the fact that $(qI_n-T_w)(qI_n-T_w)^{-1}=I_n$, we obtain that $\mathbf{e}_i=y_{1i}\mathbf{x}_1^w+\ldots+y_{ni}\mathbf{x}_n^w$ where $\mathbf{x}_i^w$ are the columns of the matrix $(qI_n-T_w)^{-1}$. Thus there is an isomorphism induced by the map $\mathbf{x}_i^w\pmod{\mathbf{Z}^n}\mapsto\mathbf{e}_i\pmod{\mathrm{Col}(qI_n-T_w)}$.

We immediately see from the above isomorphism that $|X(w)|=\det|qI_n-T_w|$. However, it is relatively harder to obtain the cardinality of the set $kX(w)$ for $k>1$ because this quantity is related with the structure of $X(w)$. The structure of $X(w)\cong\mathbf{Z}^n/\mathrm{Col}(qI_n-T_w)$ can be obtained by the Smith normal form of the matrix qI_n-T_w. Since $\mathbf{Z}$ is a principal ideal domain, the Smith normal form exists and it is a diagonal matrix with entries $(1,\ldots,1,a_1,\ldots,a_m)$ for some unique positive integers $a_1|a_2|\cdots|a_m$. We have $X(w)\cong C_{a_1}\times\cdots\times C_{a_m}$ for cyclic groups C_{a_i} of order a_i. We define the quantity

$$d(k,w)=\prod_{i=1}^{m}\frac{a_i}{\gcd(k,a_i)}.$$

Obviously $|kX(w)|=d(k,w)$ for each positive integer k. For example, $d(1,w)=|X(w)|$ for each $w\in W$. On the other hand, $d(a_m,w)=1$ for each $w\in W$.

Lemma 2.1 *If w_1 and w_2 are in the same conjugacy class in W, then the Smith normal forms of matrices $qI_n-T_{w_1}$ and $qI_n-T_{w_2}$ over $\mathbf{Z}$ are the same.*

Proof Suppose that $U(qI_n-T_{w_1})V$ is the Smith normal form of $qI_n-T_{w_1}$ over $\mathbf{Z}$ for some unimodular matrices U and V with integer components. Suppose also that $w^{-1}w_1w=w_2$ for some $w\in W$. Then

$$\begin{aligned}UT_{w_1}V&=T_w^{-1}(UT_{w_1}V)T_w\\&=T_w^{-1}U(T_wT_w^{-1})T_{w_1}(T_wT_w^{-1})VT_w\\&=\tilde{U}T_{w_2}\tilde{V}.\end{aligned}$$

The matrices $\tilde{U}$ and $\tilde{V}$ are unimodular matrices with integer components. This finishes the proof since

$$U(qI_n-T_{w_1})V=UqI_nV-\tilde{U}T_{w_2}\tilde{V}=\tilde{U}(qI_n-T_{w_2})\tilde{V}.$$

□

The Weyl group W naturally acts on $\mathcal{X}$. The action of w on $\mathbf{x}$ is given by the left-multiplication map, i.e. by $T_w\mathbf{x}$. In order to prove our main result, we will use the orbit-stabilizer formula. For this purpose, we shall consider the following lemma and its generalization.

Lemma 2.2 *If $\mathbf{x} \in X(w_1)$ and $T_{w_2}\mathbf{x} \equiv \mathbf{x}$, then $\mathbf{x} \in X(w_1w_2)$.*

Proof Recall that $X(w_1)$ is defined to be the subgroup of $\mathbf{Q}^n/\mathbf{Z}^n$ generated by the columns of the matrix $(qI_n - T_{w_1})^{-1}$. Thus, we have $\mathbf{x} \in X(w_1)$ if and only if $T_{w_1}\mathbf{x} = q\mathbf{x}$ modulo $\mathbf{Z}^n$. If $T_{w_2}\mathbf{x} = \mathbf{x}$ modulo $\mathbf{Z}^n$, then

$$T_{w_1}T_{w_2}\mathbf{x} = T_{w_1}\mathbf{x} = q\mathbf{x}.$$

Since $T_{w_1}T_{w_2} = T_{w_1w_2}$, we have $\mathbf{x} \in X(w_1w_2)$. □

The Weyl group W also acts on $k\mathcal{X}$ because the scalar matrices kI_n commute with each T_w. The following generalization of the previous lemma is the key argument to prove the equality part of our main result.

Lemma 2.3 *Let k be a positive integer such that $\gcd(k, |W|) = 1$. If $\mathbf{x} \in kX(w_1)$ and $T_{w_2}\mathbf{x} \equiv \mathbf{x}$, then $\mathbf{x} \in kX(w_1w_2)$.*

Proof Let $\mathbf{x}$ be an element of $kX(w_1)$, then there exists $\mathbf{y} \in X(w_1)$ such that $\mathbf{x} = k\mathbf{y}$. Moreover, $T_{w_1}\mathbf{y} \equiv q\mathbf{y}$ modulo $\mathbf{Z}^n$. Our purpose is to construct $\mathbf{y}' \in X(w_1w_2)$ such that $\mathbf{x} = k\mathbf{y}'$

We start with writing $X(w_1) = H_1 \oplus H_2$ as a direct sum of groups H_1 and H_2 so that the prime divisors of $|H_1|$ are divisors of $|W|$ and $\gcd(|H_2|, |W|) = 1$. This decomposition enables us to use the condition $\gcd(k, |W|) = 1$. We write $\mathbf{y} = \mathbf{y}_1 + \mathbf{y}_2$ with unique $\mathbf{y}_i \in H_i$.

Let s be the order of w_2 in W. Suppose that $s\tilde{s} \equiv 1 \pmod{|H_2|}$ for some integer $\tilde{s}$. Now we consider

$$\mathbf{y}' = \mathbf{y}_1 + \tilde{s}(T_{w_2}^{s-1} + \ldots + T_{w_2} + I_n)\mathbf{y}_2.$$

Suppose that $T_{w_2}\mathbf{x} \equiv \mathbf{x}$. Clearly, $T_{w_2}k\mathbf{y}_i = k\mathbf{y}_i$ for each i. The multiplication by k restricted to H_1 is injective. It follows that $T_{w_2}\mathbf{y}_1 = \mathbf{y}_1$. It is now obvious that $T_{w_2}\mathbf{y}' = \mathbf{y}'$ and $\mathbf{y}' \in X(w_1)$. Lemma 2.2 implies that $\mathbf{y}' \in X(w_1w_2)$. Moreover,

$$\begin{aligned} k\mathbf{y}' &= k\mathbf{y}_1 + \tilde{s}(T_{w_2}^{s-1} + \ldots + T_{w_2} + I_n)k\mathbf{y}_2 \\ &= k\mathbf{y}_1 + \tilde{s}sk\mathbf{y}_2 \\ &= k\mathbf{y}_1 + k\mathbf{y}_2 \\ &= \mathbf{x}. \end{aligned}$$

This finishes the proof. □

The stabilizer subgroup of W with respect to $\mathbf{x} \in k\mathcal{X}$ is defined by

$$W_{\mathbf{x}} = \{w \in W : T_w\mathbf{x} = \mathbf{x}\}.$$

The number of elements in the orbit $W\mathbf{x}$ is found by the orbit-stabilizer formula. More precisely, we have

$$|W\mathbf{x}| = \frac{|W|}{|W_{\mathbf{x}}|}.$$

Let $\{w_1W_{\mathbf{x}}, \ldots, w_mW_{\mathbf{x}}\}$ be representatives for the cosets in $W/W_{\mathbf{x}}$. Suppose that $\mathbf{x} \in X(w)$. For each coset $w_iW_{\mathbf{x}}$, we associate the element $\mathbf{x}_i = T_{w_i}\mathbf{x} \in X(w)$. In this fashion we obtain a subset $\{\mathbf{x}_1, \ldots, \mathbf{x}_m\} \subseteq X(w)$ with precisely m elements. Moreover, $\Phi_{\mathfrak{g}}(\mathbf{x}_i) = \Phi_{\mathfrak{g}}(\mathbf{x}_j)$ for all $1 \leq i, j \leq m$.

We are now ready to prove our main result.

Theorem 2.4 *Let q be a power of a prime p and suppose that $p > n$. Let $\mathfrak{g}$ be a semisimple complex Lie algebra of rank n and let W be its Weyl group. Let $\{\mathfrak{c}_1, \ldots, \mathfrak{c}_m\}$ be the conjugacy classes in W with representatives $w_i \in \mathfrak{c}_i$ for each i. For any positive integer k, we have*

$$\left|P_{\mathfrak{g}}^k(\mathbf{F}_q^n)\right| \geq \frac{1}{|W|}\sum_{i=1}^{m} |\mathfrak{c}_i| d(k, w_i).$$

The equality holds if $\gcd(k, |W|) = 1$.

Proof Recall that we have the following one-to-one correspondences

$$\mathcal{X}/\sim \longleftrightarrow \mathrm{Fix}(P_{\mathfrak{g}}^q) \longleftrightarrow \mathbf{F}_q^n.$$

In order to count the number of elements in $P_{\mathfrak{g}}^k(\mathbf{F}_q^n)$, it is enough to count the elements in the quotient set $(k\mathcal{X})/\sim$. We have

$$k\mathcal{X} = k\left(\bigcup_{w\in W} X(w)\right) = \bigcup_{w\in W} kX(w).$$

Recall that $kX(w)$ has order $d(k, w)$. We consider the sum $\sum_{w\in W} d(k, w)$ and focus on the equivalence classes $[\mathbf{x}] \in (k\mathcal{X})/\sim$. We claim that each equivalence class is counted at most $|W|$ times within this sum.

Let $[\mathbf{x}]$ be an equivalence class in $(k\mathcal{X})/\sim$ with $\mathbf{x} \in kX(w)$ for some $w \in W$. Suppose that the stabilizer subgroup $W_{\mathbf{x}}$ has order ℓ and suppose that $W/W_{\mathbf{x}}$ has order m. By the orbit-stabilizer formula, $|W| = \ell \cdot m$. We have $\mathbf{x} \in kX(w)$. If $\mathbf{x} \in kX(w\tilde{w})$ for some $\tilde{w} \in W$, then we claim that $T_{\tilde{w}}\mathbf{x} = \mathbf{x}$. To see this, we note

$$T_w(T_{\tilde{w}}\mathbf{x} - \mathbf{x}) = T_wT_{\tilde{w}}\mathbf{x} - T_w\mathbf{x} = q\mathbf{x} - q\mathbf{x} = \mathbf{0}$$

In such a case, we have $\tilde{w} \in W_{\mathbf{x}}$. From this, we obtain that $\mathbf{x} \in kX(w)$ holds for at most ℓ different $w \in W$. Moreover, there are m distinct representatives of the equivalence class $[\mathbf{x}]$ in each $kX(w\tilde{w})$. This proves the claim that each equivalence class $[\mathbf{x}] \in (k\mathcal{X})/\sim$ is counted at most $|W|$ times within the sum $\sum_{w\in W} d(k, w)$.

The value $d(k, w)$ is identical for group elements in the same conjugacy class by Lemma 2.1. That's why we have

$$\sum_{w\in W} d(k, w) = \sum_{i=1}^{m} |\mathfrak{c}_i| d(k, w_i).$$

This finishes the proof of the inequality part of the theorem.

Now suppose that $\gcd(k, |W|) = 1$. In addition to the previous picture, now we can use Lemma 2.3. For each $\tilde{w} \in W_{\mathbf{x}}$, we have $\mathbf{x} \in X(w\tilde{w})$. This proves the fact that each equivalence class $[\mathbf{x}] \in (k\mathcal{X})/\sim$ is counted precisely $|W|$ times within the sum $\sum_{w\in W} d(k, w)$. □

Note that the main result of [5], which is valid only for $n = 2$, is slightly stronger than this theorem. For the semisimple Lie algebras, A_2, B_2, and G_2, that result gives a precise value for $\left|P^k_{\mathfrak{g}}(\mathbf{F}^n_q)\right|$ without any restriction on k.

3. An example

We finish our paper by giving an example. Let $\mathfrak{g} = B_2$ and let $\{\alpha_1, \alpha_2\}$ be a choice of simple roots. The Weyl group W is generated by the reflections s_{α_1} and s_{α_2}. The action of the Weyl group over the root system is determined by the Cartan matrix

$$A = \begin{bmatrix} 2 & -1 \\ -2 & 2 \end{bmatrix}.$$

The transpose of the Cartan matrix transforms the fundamental weights to the fundamental roots, i.e. $\alpha_i = \sum_{j=1}^{n} A_{ji}\omega_j$. We have

$$T_{w_1} = \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} \quad \text{and} \quad T_{w_2} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}.$$

The Weyl group W is isomorphic to the dihedral group of order 8. We use the classical representation of this group for the convenience of the reader. Set $a = T_{w_1}T_{w_2}$ and $x = T_{w_1}$. Note that the order of a is 4 and $xax^{-1} = a^{-1}$. We have $W = \{a^i x^j : 0 \le i \le 3, 0 \le j \le 1\}$. There are five conjugacy classes. Set

$\mathfrak{c}_1$	$\mathfrak{c}_2$	$\mathfrak{c}_3$	$\mathfrak{c}_4$	$\mathfrak{c}_5$
id	a^2	x, a^2x	ax, a^3x	a, a^3.

We find that

$$(qI_n - \mathrm{id})^{-1} = \begin{bmatrix} \frac{1}{q-1} & 0 \\ 0 & \frac{1}{q-1} \end{bmatrix} \quad \text{and} \quad (qI_n - a^2)^{-1} = \begin{bmatrix} \frac{1}{q+1} & 0 \\ 0 & \frac{1}{q+1} \end{bmatrix}$$

The columns of these matrices are independent from each other and they generate abelian groups of orders $(q-1)^2$ and $(q+1)^2$, respectively.

The elements x and a^2x are in the same conjugacy class and the columns of the corresponding matrices generate abelian groups of size $q^2 - 1$.

$$(qI_n - x)^{-1} = \begin{bmatrix} \frac{1}{q+1} & 0 \\ \frac{2}{q^2-1} & \frac{1}{q-1} \end{bmatrix} \quad \text{and} \quad (qI_n - a^2x)^{-1} = \begin{bmatrix} \frac{1}{q-1} & 0 \\ \frac{-2}{q^2-1} & \frac{1}{q+1} \end{bmatrix}$$

The elements ax and a^3x are in the same conjugacy class and the columns of the corresponding matrices generate abelian groups of size $q^2 - 1$.

$$(qI_n - ax)^{-1} = \begin{bmatrix} \frac{1}{q+1} & \frac{-1}{q^2-1} \\ 0 & \frac{1}{q-1} \end{bmatrix} \quad \text{and} \quad (qI_n - a^3x)^{-1} = \begin{bmatrix} \frac{1}{q-1} & \frac{1}{q^2-1} \\ 0 & \frac{1}{q+1} \end{bmatrix}$$

Finally, the elements a and a^3 are in the same conjugacy class and the columns of the corresponding matrices generate abelian groups of size $q^2 + 1$.

$$(qI_n - a)^{-1} = \begin{bmatrix} \frac{q-1}{q^2+1} & \frac{-1}{q^2+1} \\ \frac{2}{q^2+1} & \frac{q+1}{q^2+1} \end{bmatrix} \quad \text{and} \quad (qI_n - a^3)^{-1} = \begin{bmatrix} \frac{q+1}{q^2+1} & \frac{1}{q^2+1} \\ \frac{-2}{q^2+1} & \frac{q-1}{q^2+1} \end{bmatrix}.$$

Let us pick a representative $w_i \in \mathfrak{c}_i$ for each conjugacy class. The Weyl group W has order eight and there are five conjugacy classes in W. Set

$$N = \frac{1}{8}\sum_{i=1}^{5} |\mathfrak{c}_i| d(k, w_i).$$

If we fix $q = 3$, then we obtain the following table:

k	$d(w_1,k)$	$d(w_2,k)$	$d(w_3,k)$	$d(w_4,k)$	$d(w_5,k)$	N
1	4	16	8	8	10	9
2	1	4	2	4	5	7/2
5	4	16	8	8	2	7

The integers $k = 1$ and $k = 5$ are relatively prime to 8. Thus, the quantity N is precisely the cardinality of the value set of the folding polynomial $P^k_{B_2}$. On the other hand, the integer $k = 2$ is not relatively prime to 8. Our main result in this paper implies that $\left|P^2_{B_2}(\mathbf{F}_3^2)\right| \geq 7/2$. Indeed, we have $\left|P^2_{B_2}(\mathbf{F}_3^2)\right| = 5$ by the slightly stronger result in [5].

References

[1] Chevalley C. Invariants of finite groups generated by reflections. American Journal of Mathematics 1955; 77: 778-782.

[2] Chou WS, Gomez-Calderon J, Mullen GL. Value sets of Dickson polynomials over finite fields.Journal of Number Theory 1988; 30(3): 334-344.

[3] Hoffman ME, Withers WD. Generalized Chebyshev polynomials associated with affine Weyl groups. Transactions of the American Mathematical Society 1988; 308: 91-104.

[4] Küçüksakallı Ö. Value sets of bivariate Chebyshev maps over finite fields. Finite Fields and Their Applications 2015; 36: 189-202.

[5] Küçüksakallı Ö. Value sets of bivariate folding polynomials over finite fields. Finite Fields and Their Applications 2018; 54: 253-272.

[6] Küçüksakallı Ö. On the arithmetic exceptionality of polynomial mappings. Bulletin of the London Mathematical Society 2018; 50: 143-147.

[7] Mullen GL, Wan D, Wang Q. Value sets of polynomial maps over finite fields. Quarterly Journal of Mathematics 2013; 64 (4): 1191-1196.

[8] Veselov AP. Integrable mappings and Lie algebras. Soviet Mathematics - Doklady 1987; 35: 211-213.

[9] Withers WD. Folding polynomials and their dynamics. American Mathematical Monthly 1988; 95 (5): 399-413.