Value sets of folding polynomials over finite fields

Ömer KÜÇÜKSÄKALLI∗
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 \( g \). We find the cardinality of the value sets of the folding polynomials \( P^k_g(x) \in \mathbb{Z}[x] \) 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 \( F_p \) be a finite field of characteristic \( p \). Given a polynomial \( f(x) \in \mathbb{Z}[x_1, \ldots, x_n] \), we consider the induced map \( f : F_p^n \to F_p^n \). The problem of finding the cardinality of the value set \( f(F_p^n) = \{f(x) : x \in F_p^n\} \) 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 \( P^k_{A_1} \) 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 \( P^k_{A_2} \) in [4] and extended the idea for the polynomials \( P^k_{B_2} \) and \( P^k_{G_2} \) 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 \( P^k_g \) are associated with semisimple complex Lie algebras and we need some notation to describe these polynomials. Let \( g \) 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 \( \Phi_\mathfrak{h} : \mathfrak{h}/L \to \mathbb{C}^n \), induced from the action of \( W \) on \( \mathcal{L} \), where \( \Phi_\mathfrak{h} = (\varphi_1, \ldots, \varphi_n) \)

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

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

This work is licensed under a Creative Commons Attribution 4.0 International License.
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 $P_k^{\mathfrak{g}}$, $k \in \mathbb{N}$ determined from the conditions

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

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

For a semisimple complex Lie algebra $\mathfrak{g}$ of rank $n$ with roots $\lambda_i$, $i = 1, \ldots, n$, we identify $\mathfrak{h} = \mathbb{C}\lambda_i$ (respectively the lattice $L = \oplus\mathbb{Z}\lambda_i$) with $\mathbb{C}^n$ (respectively $\mathbb{Z}^n$). For $w \in W$, $T_w$ is the $n \times n$ matrix representing the endomorphism $T_w : L \rightarrow L$ 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 $q^2$ is not a root of unity. The matrix $qI_n - T_w$ and its inverse are the main tools to study the polynomial mappings $P_k^{\mathfrak{g}}$.

**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 $P_k^{\mathfrak{g}} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ 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 $\mathbb{F}_q^n$ 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 $\zeta$ be a primitive root of unity of order $p^e - 1$. Let $p$ be a prime ideal of the cyclotomic extension $\mathbb{Q}(\zeta)$ lying over $p$. There is a one-to-one correspondence

$$\Fix(P_\mathfrak{g}^n) \longleftrightarrow \mathbb{F}_q^n$$

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

$$X(w) := \text{Col}((qI_n - T_w)^{-1})/\mathbb{Z}^n$$

as a subgroup of $\mathbb{Q}^n/\mathbb{Z}^n$. 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 $\Fix(P_\mathfrak{g}^n)$, and therefore all the elements in $\mathbb{F}_q^n$, with an $n$-tuple from $\mathbb{Q}^n/\mathbb{Z}^n$. More precisely, we have a surjective function

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

$$X/\sim \leftrightarrow \text{Fix}(P_q^g) \leftrightarrow F_q^n.$$ 

After this brief summary of [6], we are now ready to study the value set $P_q^k(F_q^n)$ by using $(kX)/\sim$.

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

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

To justify this, we denote the columns of $qI_n - T_w$ by $y^w_i = (y_{1i}, \ldots, y_{ni})$. Using the elementary column vectors $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$, we can write $y^w_i = y_{1i}e_1 + \ldots + y_{ni}e_n$. On the other hand, using the fact that $(qI_n - T_w)(qI_n - T_w)^{-1} = I_n$, we obtain that $e_i = y_{1i}x^w_i + \ldots + y_{ni}x^w_n$ where $x^w_i$ are the columns of the matrix $(qI_n - T_w)^{-1}$. Thus there is an isomorphism induced by the map $x^w_i \mod \text{Col}(qI_n - T_w) \mapsto e_i$.

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 $X(w) \cong Z^n/\text{Col}(qI_n - T_w)$ can be obtained by the Smith normal form of the matrix $qI_n - T_w$. Since $Z$ 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, $d(a_i, w) = 1$ 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 $Z$ 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 $Z$ 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

$$UT_{w_1}V = T_{w_1}^{-1}(UT_{w_1}V)T_{w_2} = T_{w_1}^{-1}U(T_wT_{w_1}^{-1})T_{w_1}(T_wT_{w_1}^{-1})VT_{w_2} = \hat{U}T_{w_2}\hat{V}.$$ 

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

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

\[ \square \]
The Weyl group $W$ naturally acts on $\mathcal{X}$. The action of $w$ on $x$ is given by the left-multiplication map, i.e. by $T_w x$. 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 $x \in X(w_1)$ and $T_{w_2}x \equiv x$, then $x \in X(w_1w_2)$.

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

$$T_{w_1}T_{w_2}x = T_{w_2}x = qx.$$ 

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

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 $x \in kX(w_1)$ and $T_{w_2}x \equiv x$, then $x \in kX(w_1w_2)$.

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

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 $y = y_1 + y_2$ with unique $y_i \in H_i$.

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

$$y' = y_1 + s(T_{w_2}^{-1} + \ldots + T_{w_2} + I_n)y_2.$$ 

Suppose that $T_{w_2}x \equiv x$. Clearly, $T_{w_2}ky_i = ky_i$ for each $i$. The multiplication by $k$ restricted to $H_1$ is injective. It follows that $T_{w_2}y_1 = y_1$. It is now obvious that $T_{w_2}y' = y'$ and $y' \in X(w_1)$. Lemma 2.2 implies that $y' \in X(w_1w_2)$. Moreover,

$$ky' = ky_1 + \bar{s}(T_{w_2}^{-1} + \ldots + T_{w_2} + I_n)ky_2 = ky_1 + \bar{s}ky_2 = ky_1 + ky_2 = x.$$

This finishes the proof. \hfill $\square$

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

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

The number of elements in the orbit $Wx$ is found by the orbit-stabilizer formula. More precisely, we have

$$|Wx| = \frac{|W|}{|W_x|}.$$
Let \( \{w_1 W_x, \ldots, w_m W_x\} \) be representatives for the cosets in \( W/W_x \). Suppose that \( x \in X(w) \). For each coset \( w_i W_x \), we associate the element \( x_i = T_{w_i} x \in X(w) \). In this fashion we obtain a subset \( \{x_1, \ldots, x_m\} \subseteq X(w) \) with precisely \( m \) elements. Moreover, \( \Phi_g(x_i) = \Phi_g(x_j) \) 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 \( \{c_1, \ldots, c_m\} \) be the conjugacy classes in \( W \) with representatives \( w_i \in c_i \) for each \( i \). For any positive integer \( k \), we have

\[
|P^k_{\mathfrak{g}}(F_q^n)| \geq \frac{1}{|W|} \sum_{i=1}^m |c_i|d(k, w_i).
\]

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

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

\[
\mathcal{X}/\sim \leftrightarrow \text{Fix}(P^q_{\mathfrak{g}}) \leftrightarrow F_q^n.
\]

In order to count the number of elements in \( P^k_{\mathfrak{g}}(F_q^n) \), 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 \([x] \in (k\mathcal{X})/\sim\). We claim that each equivalence class is counted at most \(|W|\) times within this sum.

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

\[
T_{w}(T_{\tilde{w}}x - x) = T_wT_{\tilde{w}}x - T_wx = qx - qx = 0
\]

In such a case, we have \( \tilde{w} \in W_x \). From this, we obtain that \( x \in kX(w) \) holds for at most \( \ell \) different \( w \in W \). Moreover, there are \( m \) distinct representatives of the equivalence class \([x] \) in each \( kX(w\tilde{w}) \). This proves the claim that each equivalence class \([x] \in (k\mathcal{X})/\sim\) 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

\[
\sum_{w \in W} d(k, w) = \sum_{i=1}^m |c_i|d(k, w_i).
\]

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 \( \tilde{w} \in W_x \), we have \( x \in X(w\tilde{w}) \). This proves the fact that each equivalence class \([x] \in (k\mathcal{X})/\sim\) is counted precisely \(|W|\) times within the sum \( \sum_{w \in W} d(k, w) \). \( \square \)
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 \( |P_k^q(F_n^q)| \) without any restriction on \( k \).

3. An example

We finish our paper by giving an example. Let \( g = B_2 \) and let \( \{\alpha_1, \alpha_2\} \) be a choice of simple roots. The Weyl group \( W \) is generated by the reflections \( s_{\alpha_1} \) and \( s_{\alpha_2} \). 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. \( \alpha_i = \sum_{j=1}^n A_{ij} \omega_j \). 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 \( W = \{a^i x^j : 0 \leq i \leq 3, 0 \leq j \leq 1\} \). There are five conjugacy classes. Set

\[
\begin{array}{|c|c|c|c|c|}
\hline
\epsilon_1 & \epsilon_2 & \epsilon_3 & \epsilon_4 & \epsilon_5 \\
\hline
\text{id} & a^2 & x, a^2x & ax, a^3x & a, a^3 \\
\hline
\end{array}
\]

We find that

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

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 \( a^2 x \) are in the same conjugacy class and the columns of the corresponding matrices generate abelian groups of size \( q^2 - 1 \).

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

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

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

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 \( q^2 + 1 \).

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

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

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

<table>
<thead>
<tr>
<th>$k$</th>
<th>$d(w_1, k)$</th>
<th>$d(w_2, k)$</th>
<th>$d(w_3, k)$</th>
<th>$d(w_4, k)$</th>
<th>$d(w_5, k)$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>$7/2$</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>2</td>
<td>7</td>
</tr>
</tbody>
</table>

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 $P_{B_2}^k$. On the other hand, the integer $k = 2$ is not relatively prime to 8. Our main result in this paper implies that $|P_{B_2}^2(F_3^2)| \geq 7/2$. Indeed, we have $|P_{B_2}^2(F_3^2)| = 5$ by the slightly stronger result in [5].

References