ON THE ARITHMETIC EXCEPTIONALITY OF POLYNOMIAL MAPPINGS

ÖMER KÜÇÜKSAKALLI

Abstract. In this note we prove that certain polynomial mappings $P_{\mathfrak{g}}^k(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}]$ in n-variables obtained from simple complex Lie algebras $\mathfrak{g}$ of arbitrary rank $n \geq 1$, are exceptional.

We recall that a polynomial mapping $P \in \mathbf{Z}[\mathbf{x}]$ in n variables is said to be exceptional if the reduced map $\bar{P} : \mathbf{F}_p^n \to \mathbf{F}_p^n$ is a permutation for infinitely many primes p. Lidl and Wells proved the existence of nontrivial exceptional polynomial mappings of arbitrary rank [LW72]. They achieved this by means of elementary methods, namely using the theory of symmetric functions, however their construction can be related to the simple complex Lie algebras A_n [HW88].

In this paper, we prove that certain polynomial mappings $P_{\mathfrak{g}}^k(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}]$ in n-variables obtained from arbitrary simple complex Lie algebras $\mathfrak{g}$ of rank $n \geq 1$ are exceptional. The structure of the proof follows closely the pattern of the $n = 2$ case [Kü16].

Let $\mathfrak{g}$ be a simple 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 $\omega_1, \dots, \omega_n$, and L the dual lattice in $\mathfrak{h}$. Applying the exponential form of Chevalley's Theorem (Thm. 1, p.188, [GAL]) one proves that the quotient of $\mathfrak{h}/L$ under the action of the Weyl group W (induced from the action of W on $\mathcal{L}$) is the n-dimensional complex affine space and the quotient map is given by $\Phi_{\mathfrak{g}} : \mathfrak{h}/L \to \mathbf{C}^n$, $\Phi_{\mathfrak{g}} = (\varphi_1, \dots, \varphi_n)$

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

This construction leads to the following result first given by Veselov, and somewhat later by Hofmann and Withers independently.

Theorem 1 ([Ve87],[HW88])**.** *With each simple 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.

We will prove that for any $\mathfrak{g}$, there exists k such that the mapping $P_{\mathfrak{g}}^k$ is exceptional (Corollary 4).

We first fix our notation.

Date: October 21, 2018.
2010 *Mathematics Subject Classification.* 11T06.
Key words and phrases. keywords.

Throughout the paper q denotes a power of a prime p.

Frob_q is the Frobenius map $(x_1, \ldots, x_n) \mapsto (x_1^q, \ldots, x_n^q)$.

For any polynomial $P \in \mathbf{Z}[\mathbf{x}]$ in the n variables $x_1, \ldots, x_n$, $\bar{P} : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is the map induced by reduction mod p.

$\mathbf{K} = \mathbf{Q}(\text{Fix}(P_{\mathfrak{g}}^q))$ is the number field which is obtained by adjoining the coordinates of the fixed points of $P_{\mathfrak{g}}^q$ to the rational numbers.

$\mathfrak{p}$ is a prime ideal of $\mathbf{K}$ lying over p.

For $\mathfrak{g}$ a simple complex Lie algebra of rank n with roots λ_i, $i = 1, \ldots, n$ we identify $\mathfrak{h} = \oplus \mathbf{C}\lambda_i$ (resp. the lattice $L = \oplus \mathbf{Z}\lambda_i$) with $\mathbf{C}^n$ (resp. $\mathbf{Z}^n$).

I_n is the identity matrix of dimensions $n \times n$. For $w \in W$, T_w is the $n \times n$ matrix representing the endomorphism $T_w : \mathcal{L} \to \mathcal{L}$ defined by $T_w(\omega_i) = w(\omega_i)$ for each $i = 1, \ldots, n$.

The following commutative diagram summarizes the set-up we will work in.

$$\begin{array}{ccc} \mathfrak{h}/L & \xrightarrow{\quad \Phi_{\mathfrak{g}} \quad} & \mathbf{C}^n \\ {\scriptstyle [\mathrm{k}]}\downarrow & & \downarrow {\scriptstyle P_{\mathfrak{g}}^k} \\ \mathfrak{h}/L & \xrightarrow{\quad \Phi_{\mathfrak{g}} \quad} & \mathbf{C}^n \end{array}$$

With this notation, our main result is the following theorem.

Theorem 2. *Let $\mathfrak{g}$ be a complex Lie algebra of rank n and let W be its Weyl group. The polynomial mapping $\bar{P}_{\mathfrak{g}}^k : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is a permutation if and only if $qI_n - T_w$ is invertible modulo k for each $w \in W$.*

The proof of the theorem will be given at the end of the paper. We note the following corollaries.

Corollary 3. *Let $\mathfrak{g}$ be a complex Lie algebra of rank n and let W be its Weyl group. The polynomial mapping $\bar{P}_{\mathfrak{g}}^k : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is a permutation if* $\gcd(k, q^s - 1) = 1$ *for each* $s \in \{\text{order of } w \mid w \in W\}$.

Proof. The matrix T_w satisfies $T_w^s = I_n$ where s is the order of $w \in W$. The matrix $(q^s - 1)I_n$ is invertible modulo k by the hypothesis. Note that

$$(q^s - 1)I_n = (qI_n)^s - T_w^s = (qI_n - T_w)(q^{s-1}I_n + \ldots + T_w^{s-1}).$$

Thus $qI_n - T_w$ is invertible modulo k. □

In Corollary 3 the converse implication is not true. Lidl and Wells prove in [LW72] that $P_{A_4}^k$ is a permutation of $\mathbf{F}_q^4$ if and only if $\gcd(k, q^s - 1) = 1$ for $s = 1, 2, 3, 4, 5$. On the other hand, the Weyl group A_4 is the symmetric group S_5 which contains an element of order 6.

An important application of Theorem 2 is the following corollary.

Corollary 4. *There exists $k \in \mathbf{N}$ such that $P_{\mathfrak{g}}^k$ is exceptional.*

Proof. There exist infinitely many primes in any arithmetic progression. It is now easy to see by Corollary 3 that for each $\mathfrak{g}$, there exists an integer k so that $P_{\mathfrak{g}}^k$ is exceptional. □

In the proof of the theorem we will need the following lemmata.

Lemma 5. *For any integer $k \geq 1$, we have $|\mathrm{Fix}(P_{\mathfrak{g}}^k)| = k^n$.*

Proof. In order to prove this lemma, we generalize an idea of Uchimura for the case $\mathfrak{g} = A_2$ [Uc09]. For an illustration of this idea, see [Kü16].

The set of points in $\mathbf{C}^n$ with bounded orbit under $P_{\mathfrak{g}}^k$ are of the form $\Phi_{\mathfrak{g}}(\mathbf{x})$ where $\mathbf{x}$ has real components. The Weyl group W acts on the quotient set $D = \mathbf{R}^n/\mathbf{Z}^n$. The elements in $\Phi_{\mathfrak{g}}(D)$ can be represented by several different expressions $\Phi(\mathbf{x})$, with $\mathbf{x} = (x_1, \ldots, x_n)$ and $0 \leq x_i < 1$, thanks to the action of the Weyl group W. Consider the compact set D/W. The multiplication map $[k] : D/W \to D/W$ induces a k^n to 1 map.

Divide D/W into k^n simplexes $T_1, \ldots, T_{k^n}$ such that each one of them is mapped onto D/W under the multiplication by k. Consider the inverse map from D/W to T_i which is division by k together with a suitable linear translation. Being a continuous map there exists at least one fixed point of this map. Moreover there is at most one such point in each T_i because of the linearity. We must show that these fixed points are distinct. A repetition can occur only at the boundaries of the simplexes T_i. However the multiplication by k maps such a boundary to the boundary of D/W. It follows that a possible repetition may only be at a corner of a simplex which has a part on the boundary of D/W. However such a corner is mapped to a corner of D/W.

It remains to show that a common corner P of two different simplexes T_i and T_j, which is at the same time a corner of D/W, is not fixed under $[k]$. Assume otherwise. The compact set D/W, and therefore each simplex, has n edges connecting to a corner. Thus, we see that there must be a common edge of T_i and T_j with endpoint P, and which does not lie on the boundary of D/W. Note that the outer n edges on the boundary of D/W should be permuted among themselves under $[k]$. On the other hand, the extra edge shall be mapped to the boundary of D/W onto one of the outer edges. Now, T_i has n edges with endpoint P, and at least two of them are mapped onto the same edge of D/W. This is a contradiction. □

Lemma 6. *Let $k \geq 1$ be an integer. The number field $\mathbf{Q}(\mathrm{Fix}(P_{\mathfrak{g}}^k))$ is contained in the compositum of the cyclotomic fields $\mathbf{Q}(\zeta_{k^s-1})$ where $s \in \{\text{order of } w \mid w \in W\}$.*

Proof. Let $\alpha = \Phi_{\mathfrak{g}}(\mathbf{x})$ be an element that is fixed under $P_{\mathfrak{g}}^k$. It follows that $k\mathbf{x} \equiv w\mathbf{x} \pmod{\mathbf{Z}^n}$ for some $w \in W$. If the order of w is s, then we have $k^s\mathbf{x} \equiv \mathbf{x} \pmod{\mathbf{Z}^n}$. It follows that $\mathbf{x}$ is a vector with rational components whose denominators are divisors of $k^s - 1$. □

Lemma 7. *Let α and β be elements of $\mathrm{Fix}(P_{\mathfrak{g}}^q)$. If $\alpha \equiv \beta \pmod{\mathfrak{p}}$, then $\alpha = \beta$.*

Proof. There exist $\mathbf{a}, \mathbf{b} \in \mathcal{O}_{\mathfrak{p}}^n/\mathbf{Z}^n$, where $\mathcal{O}_{\mathfrak{p}}$ is the localization at $\mathfrak{p}$ of the ring of integers $\mathcal{O}$ of $\mathbf{K}$, such that $\alpha = \Phi_{\mathfrak{g}}(\mathbf{a})$ and $\beta = \Phi_{\mathfrak{g}}(\mathbf{b})$. The components of $\mathbf{a}$ and $\mathbf{b}$ have denominators which are divisors of $q^s - 1$ by the proof of Lemma 6. Note that $\zeta_{q^s-1}^m \equiv \zeta_{q^s-1}^{\tilde{m}} \pmod{\mathfrak{p}}$ if and only if $m \equiv \tilde{m} \pmod{q^s - 1}$. Moreover, the map $\Phi_{\mathfrak{g}}$ is a composition of elementary symmetric functions, invertible linear maps and maps of the form $z + 1/z$ [HW88]. If $\bar{\alpha} = \bar{\beta}$, then this means that $w_1\mathbf{a} \equiv w_2\mathbf{b} \pmod{\mathbf{Z}^n}$ for some $w_1, w_2 \in W$. Thus $\alpha = \Phi_{\mathfrak{g}}(w_1\mathbf{a}) = \Phi_{\mathfrak{g}}(w_2\mathbf{b}) = \beta$. □

Lemma 8. *We have $\bar{P}_{\mathfrak{g}}^q = \mathrm{Frob}_q$.*

Proof. Let us consider the map $\bar{\Phi}_{\mathfrak{g}} : \mathcal{O}_{\mathfrak{p}}^n/\mathbf{Z}^n \to \bar{\mathbf{F}}_p^n$ given by $\mathbf{x} \mapsto \overline{\Phi_{\mathfrak{g}}(\mathbf{x})}$. This map is surjective. Letting $t_j = e^{2\pi i x_j}, j = 1, \ldots, n$ we see that each component φ_k of

$\Phi_{\mathfrak{g}}(\mathbf{x})$ is given by a sum of integer powers of t_j's. It follows that $\varphi_k(q\mathbf{x})$ is obtained by raising each term in this sum to its q-th power. We have

$$\begin{aligned}\bar{P}_{\mathfrak{g}}^q\left(\overline{\Phi_{\mathfrak{g}}(\mathbf{x})}\right) &= \left(\overline{\varphi_1(q\mathbf{x})},\ldots,\overline{\varphi_n(q\mathbf{x})}\right)\\ &= \left(\left(\overline{\varphi_1(\mathbf{x})}\right)^q,\ldots,\left(\overline{\varphi_n(\mathbf{x})}\right)^q\right)\\ &= \mathrm{Frob}_q\left(\overline{\Phi_{\mathfrak{g}}(\mathbf{x})}\right).\end{aligned}$$

This proves the claim. □

There are q^n fixed points of $P_{\mathfrak{g}}^q$ by Lemma 5. Each one of these elements reduce to a different element in $(\mathcal{O}/\mathfrak{p})^n$ by Lemma 7. Moreover, each reduced element belongs to $\mathbf{F}_q^n$ by Lemma 8. Thus, we have a one-to-one correspondence

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

obtained by reducing the elements in $\mathrm{Fix}(P_{\mathfrak{g}}^q)$ modulo $\mathfrak{p}$. Note that $\mathcal{O}/\mathfrak{p}$ is always a nontrivial extension of $\mathbf{F}_q$. This correspondence is compatible under the actions of $\bar{P}_{\mathfrak{g}}^q$ and $P_{\mathfrak{g}}^q$, respectively.

Now, we are ready to prove our main result.

Proof. Let $\alpha = \Phi_{\mathfrak{g}}(\mathbf{x})$ be an element of $\mathrm{Fix}(P_{\mathfrak{g}}^q)$. Then, we have

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

Thus, the restricted map $P_{\mathfrak{g}}^k : \mathrm{Fix}(P_{\mathfrak{g}}^q) \to \mathrm{Fix}(P_{\mathfrak{g}}^q)$ is well-defined. The components of $\mathbf{x}$ are rational numbers whose denominators are divisors of $q^s - 1$ by the proof of Lemma 6. Actually, we can say more about these components. The set of fixed points of $P_{\mathfrak{g}}^q$ is obtained by solving the equation $q\mathbf{x} = w\mathbf{x} \pmod{\mathbf{Z}^n}$ for each $w \in W$. It is clear that the rows $\mathbf{x}_i^w$ of the matrix $(qI_n - T_w)^{-1}$ generate the set $\mathrm{Fix}(P_{\mathfrak{g}}^q)$. More precisely, we have

$$\mathrm{Fix}(P_{\mathfrak{g}}^q) = \left\{\Phi_{\mathfrak{g}}\left(\sum_{i=1}^n m_i\mathbf{x}_i^w\right) : m_i \in \mathbf{Z}, w \in W\right\}.$$

Suppose that $qI_n - T_w$ is invertible modulo k for each $w \in W$. This means that the vectors $\mathbf{x}_i^w$ have rational components whose denominators are relatively prime to k. Let d be the product of all possible denominators, when the components of $\mathbf{x}_i^w$ are expressed in their lowest terms. Then there exists ℓ such that $k\ell \equiv 1 \pmod{d}$. As a result $P_{\mathfrak{g}}^k$ and $P_{\mathfrak{g}}^\ell$, restricted to $\mathrm{Fix}(P_{\mathfrak{g}}^q)$, are inverses of each other. Therefore $P_{\mathfrak{g}}^k$ permutes the finite set $\mathrm{Fix}(P_{\mathfrak{g}}^q)$.

For the converse, suppose that $P_{\mathfrak{g}}^k$ permutes the finite set $\mathrm{Fix}(P_{\mathfrak{g}}^q)$. This is possible if the multiplication by k does not kill any denominators within the vectors $\mathbf{x}_i^w$. Therefore, the matrix $qI_n - T_w$ must be invertible modulo k for each $w \in W$. □

Veselov believes that the family of maps $P_{\mathfrak{g}}^k$ exhaust all integrable polynomial mappings $\mathbf{C}^n \to \mathbf{C}^n$ of degree $d > 1$ ([Ve87], p.212). To the best of our knowledge, no counterexample has been found so far. Relying on this conjecture, one expects that the family $P_{\mathfrak{g}}^k$ together with linear mappings exhaust all exceptional mappings in n variables.

Acknowledgement. It is a pleasure for the author to thank H. Önsiper for some useful discussions.

References

[GAL] N. Bourbaki, *Elements de Mathèmatique, Groupes et Algebres de Lie*, Hermann, Paris, 1972.

[HW88] M. E. Hoffman and W. D. Withers; *Generalized Chebyshev polynomials associated with affine Weyl groups.* Trans. Amer. Math. Soc. 308 (1988), 91–104.

[Kü16] Ö. Küçüksakallı, *Bivariate polynomial mappings associated with simple complex Lie algebras.* J. Number Theory 168 (2016), 433–451.

[LW72] R. Lidl, C. Wells, *Chebyshev polynomials in several variables.* J. Reine Angew. Math. 255 (1972), 104–111.

[Uc09] K. Uchimura, *Generalized Chebyshev maps of* $\mathbf{C}^2$ *and their perturbations.* Osaka J. Math. 46 (2009), no. 4, 995–1017.

[Ve87] A. P. Veselov, *Integrable mappings and Lie algebras.* Soviet Math. Dokl. 35 (1987), 211–213.

Middle East Technical University, Mathematics Department, 06800 Ankara, Turkey.
E-mail address: `komer@metu.edu.tr`