Bull. Aust. Math. Soc. **100** (2019), 256–267
doi:10.1017/S0004972719000340

ON THE DIMENSION OF PERMUTATION VECTOR SPACES

LUCAS REIS

(Received 9 December 2018; accepted 7 February 2019; first published online 3 April 2019)

Abstract

Let K be a field that admits a cyclic Galois extension of degree $n \geq 2$. The symmetric group S_n acts on K^n by permutation of coordinates. Given a subgroup G of S_n and $u \in K^n$, let $V_G(u)$ be the K-vector space spanned by the orbit of u under the action of G. In this paper we show that, for a special family of groups G of affine type, the dimension of $V_G(u)$ can be computed via the greatest common divisor of certain polynomials in $K[x]$. We present some applications of our results to the cases $K = \mathbb{Q}$ and K finite.

2010 *Mathematics subject classification*: primary 11T06; secondary 15A03, 20B35.

Keywords and phrases: permutation vector space, cyclic Galois extension, cyclotomic polynomial, reciprocal polynomial.

1. Introduction

Let K be a field and let $n \geq 2$ be an integer. If S_n denotes the group of permutations of $\{0, 1, \ldots, n-1\}$, there is a natural action of S_n on the K-vector space K^n. For $\delta \in S_n$ and $u = (u_0, \ldots, u_{n-1}) \in K^n$, we set $\delta(u) = (u_{\delta(0)}, \ldots, u_{\delta(n-1)})$. For $u \in K^n$, let $V_G(u)$ be the K-vector space spanned by the orbit $\{g(u) \mid g \in G\}$ of u by G and let $d_G(u)$ be the dimension of $V_G(u)$. Some natural questions arise.

(1) For $u \in K^n$, what is the value of $d_G(u)$?
(2) As u runs over K^n, what are the possible values of $d_G(u)$?
(3) If K is finite and $0 \leq r \leq n$, what is the number $N_G(r)$ of vectors $u \in K^n$ for which $d_G(u) = r$?

When $G = S_n$, it is a routine exercise to show that

$$d_{S_n}(u) = \begin{cases} 0 & \text{if } u = (0, \ldots, 0), \\ 1 & \text{if } u = (u_0, \ldots, u_0) \text{ and } u_0 \neq 0, \\ n-1 & \text{if } \sum_{i=0}^{n-1} u_i = 0 \text{ and the } u_i \text{ are not all equal}, \\ n & \text{otherwise.} \end{cases}$$

The author was supported by FAPESP Brazil, grant no. 2018/03038-2.

The main idea of the proof relies on considering $W(u) := V_{S_n}(u)^{\perp}$, the complement of $V_{S_n}(u)$, and showing that one of the vector spaces $W(u)$ or $V_{S_n}(u)$ only contains scalar multiples of the vector $v = (1, \dots, 1)$. In particular, if $K = \mathbb{F}_q$ is the finite field with q elements, where q is a power of a prime p, then

$$N_{S_n}(r) = \begin{cases} 1 & \text{if } r = 0, \\ q-1 & \text{if } r = 1, \\ q^{n-1} - c(n) & \text{if } r = n-1, \\ q^n - q^{n-1} - q + c(n) & \text{if } r = n, \\ 0 & \text{otherwise,} \end{cases}$$

where $c(n) = q$ if $n \equiv 0 \pmod p$, and $c(n) = 1$ otherwise. The proof of this enumeration formula is quite simple. We observe that $d_{S_n}(u) = n-1$ if and only if the sum of the coordinates of u equals zero and u is not of the form $(u_0, \dots, u_0)$ for some $u_0 \in \mathbb{F}_q$. In addition, the equation $x_0 + \cdots + x_{n-1} = 0$ has q^{n-1} solutions and contains exactly $c(n)$ solutions where all the variables coincide. From this fact, the numbers $N_{S_n}(r)$ for $r \neq n$ are easily computed. In addition, $N_{S_n}(n) = q^n - \sum_{r=0}^{n-1} N_{S_n}(r)$.

We identify S_n with the group of permutations of $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Under this correspondence, let $\mathbb{G}$ be the subgroup of S_n of the permutations $i \mapsto ai + b \pmod n$ of affine type. We can observe that $\mathbb{G}$ is isomorphic to $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$. In fact, the permutations $i \mapsto i + k \pmod n$ with $0 \le k < n$ form a normal subgroup of $\mathbb{G}$ (isomorphic to $\mathbb{Z}_n$) and any element of $\mathbb{G}$ can be written as a composition of a permutation $i \mapsto ai \pmod n$ with $\gcd(a, n) = 1$ (such permutations form a group isomorphic to $\mathbb{Z}_n^*$) and a permutation $i \mapsto i + k \pmod n$ with $0 \le k < n$. Moreover, if $\{a_1, \dots, a_r\}$ is a set of generators for $\mathbb{Z}_n^*$, the group $\mathbb{G}$ is generated by the permutations $\delta_{a_j} : i \mapsto a_j \cdot i \pmod n$ for $1 \le j \le r$ and the translation $\tau : i \mapsto i + 1 \pmod n$.

The main result of this paper shows that if K admits a cyclic Galois extension of degree n and G is any subgroup of $\mathbb{G}$ containing the permutation $\tau : i \mapsto i + 1 \pmod n$, we have a simple closed formula for the number $d_G(u)$, where $u \in K^n$ is arbitrary. More specifically, we prove the following theorem.

THEOREM 1.1. *Suppose that K is a field admitting a cyclic Galois extension of degree n. Let $a_1, \dots, a_s$ be positive integers and let H be the subgroup of $\mathbb{G}$ comprising the permutations $\delta_{a_j} : i \mapsto a_j \cdot i \pmod n$. For $u \in K^n$ with $u = (u_0, \dots, u_{n-1})$, set $f_u(x) = \sum_{i=0}^{n-1} i x^i$. Then, for $\tau : i \mapsto i + 1 \pmod n$ and $G = \langle \tau \rangle \rtimes H$,*

$$d_G(u) = n - \deg(M_{u,H}(x)), \tag{1.1}$$

where $M_{u,H}(x) = \gcd(x^n - 1, f_u(x^{a_1}), \dots, f_u(x^{a_s})) \in K[x]$.

On the one hand, $d_G(u)$ can always be computed after obtaining a basis for $V_G(u)$, and there are many methods to obtain such a basis. On the other hand, there are plenty of situations where Theorem 1.1 provides explicit results. For instance, if the factorisation of $x^n - 1$ over $K[x]$ is known, equation (1.1) gives the possible values of $d_G(u)$. In some cases, $d_G(u)$ is readily obtained.

Corollary 1.2. *Suppose n is a prime number and let K and G be as in Theorem 1.1. In addition, suppose that the polynomial $(x^n - 1)/(x - 1) = x^{n-1} + \cdots + x + 1$ is irreducible over K. Then $d_G(u) = d_{S_n}(u)$ for any $u \in K^n$. In particular, if K is finite, then $N_G(r) = N_{S_n}(r)$ for $0 \le r \le n$.*

The paper is structured as follows. In Section 2 we provide background material that is used along the way, including definitions and auxiliary results. In Section 3 we prove Theorem 1.1 and provide some immediate applications to the case $K = \mathbb{Q}$ and K finite. Finally, in Section 4, we explore the applicability of Theorem 1.1 to the case where G is the dihedral group D_n.

2. Preliminaries

Throughout this paper, $n \ge 2$ is a positive integer and K is a field admitting a cyclic Galois extension L of degree n. Let $\sigma : L \to L$ be any generator of $\mathrm{Gal}(L/K)$, hence σ has order n.

Definition 2.1.

(i) Let σ_0 be the identity map on L and, for each $i \ge 1$, set

$$\sigma_i = \underbrace{\sigma \circ \cdots \circ \sigma}_{i \text{ times}}.$$

(ii) Let $C(K, n) \cong K[x]/(x^n - 1)$ be the n-dimensional K-vector space comprising the polynomials $f \in K[x]$ that are constant or have degree at most $n - 1$.

The normal basis theorem (see [1]) ensures the existence of an element $z \in L$ such that $L = K(z)$ and $\{\sigma_j(z)\}_{0 \le j \le n-1}$ is a basis for L as a K-vector space. In this case, the element z is called *normal*. We fix β, a normal element of L over K.

Definition 2.2. For $f \in K[x]$ with $f(x) = \sum_{i=0}^{m} a_i x^i$ and $\alpha \in L$,

$$f \circ \alpha = \sum_{i=0}^{m} a_i \cdot \sigma_i(\alpha),$$

where the indices i are taken modulo n.

It is easy to verify that $(f \cdot g) \circ \alpha = f \circ (g \circ \alpha)$ and $(f + g) \circ \alpha = f \circ \alpha + g \circ \alpha$ for any polynomials $f, g \in K[x]$ and any $\alpha \in L$. This gives the field L a $K[x]$-module structure. In particular, for any $\alpha \in L$, the set $I_\alpha = \{g \in K[x] \mid g \circ \alpha = 0\}$ is an ideal of $K[x]$, hence is principal.

Lemma 2.3. *The ideal I_β is generated by $x^n - 1 \in K[x]$. In particular, for any $\alpha \in L$, there exists a unique $f \in C(K, n)$ such that $\alpha = f \circ \beta$.*

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

Proof. We first prove that I_β is generated by $x^n - 1$. Let F be the generator of I_β and, without loss of generality, suppose that F is monic. Since

$$(x^n - 1) \circ \beta = \sigma_0(\beta) - \sigma_0(\beta) = 0,$$

we see that F divides $x^n - 1$. If F were of degree at most $n-1$, the equality $F \circ \beta = 0$ would be a nontrivial linear combination of the elements $\{\sigma_i(\beta)\}_{0\le i\le n-1}$, with coefficients in K. This contradicts the fact that β is a normal element. Hence F has degree at least n and so $F(x) = x^n - 1$. To conclude the proof, let $\Pi : C(K, n) \to L$ be the map given by $f \mapsto f \circ \beta$. From Definition 2.2, Π is a K-linear map between K-vector spaces of dimension n. In this context, it suffices to prove that Π is onto or, equivalently, one-to-one. But $\ker(\Pi)$ is not the zero vector space if and only if I_β contains a nonzero element of $C(K, n)$, which is impossible since I_β is generated by $x^n - 1$. □

The following definitions are useful.

Definition 2.4.

(i) For $u \in K^n$ with $u = (u_0, \dots, u_{n-1})$, define $f_u(x) \in C(K, n)$ by

$$f_u(x) = \sum_{i=0}^{n-1} u_i x^i.$$

(ii) For $\delta \in S_n$ and $f \in C(K, n)$ with $f(x) = \sum_{i=0}^{n-1} a_i x^i$, we set

$$\delta(f) = \sum_{i=0}^{n-1} a_{\delta(i)} x^i.$$

It is clear that S_n acts on $C(K, n)$ via the compositions $\delta(f)$.

Example 2.5. If $f(x) = \sum_{i=0}^{n-1} a_i x^i$ and $\tau : i \mapsto i + 1 \pmod{n}$ is the translation,

$$\tau(f(x)) = a_{n-1} + \sum_{i=0}^{n-2} a_i x^{i+1}.$$

We have the following result.

Proposition 2.6. *For any subgroup J of S_n and $u \in K^n$, the space $V_J(u)$ is isomorphic to the K-vector space spanned by the set $\{\delta(f_u)\}_{\delta\in J} \subset C(K, n)$.*

Proof. For $u \in K^n$, let $W_J(u)$ and $W_J^\circ(u)$ be the K-vector spaces spanned by the sets $\{\delta(f_u)\}_{\delta\in J} \subset C(K, n)$ and $\{\delta(f_u) \circ \beta\}_{\delta\in J} \subset L$, respectively. From Lemma 2.3, the map $\Psi : K^n \to L$ given by $\Psi(v) = f_v \circ \beta$ is a K-isomorphism of K-vector spaces. Since $\Psi(V_J(u)) = W_J^\circ(u)$, it follows that $V_J(u)$ and $W_J^\circ(u)$ are isomorphic.

Let $\Gamma_u : W_J(u) \to W_J^\circ(u)$ be the K-linear map given by $\Gamma_u(g) = g \circ \beta$. From Definition 2.4, Γ_u is onto. Moreover, from Lemma 2.3, $g \circ \beta = 0$ if and only if $g(x)$ is divisible by $x^n - 1$. Since $g \in C(K, n)$ is a constant or has degree at most $n - 1$, it follows that $g = 0$, that is, $\ker \Gamma_u = \{0\}$. Therefore, $W_J(u)$ and $W_J^\circ(u)$ are isomorphic. □

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

3. A formula for $d_G(u)$ and applications

In this section we provide the proof of Theorem 1.1 and some of its immediate applications. We fix a subgroup G of $\mathbb{G}$ containing the translation τ and write $G = (\tau, H)$, where H is the unique subgroup of $\mathbb{G}$ such that G is generated by H and τ. We observe that any element of G is written uniquely as $\tau^i h$, where $0 \le i \le n-1$ and $h \in H$. In fact, G is isomorphic to the semidirect product $\langle\tau\rangle \rtimes H$, where $\langle\tau\rangle \cong \mathbb{Z}_n$ is the group generated by the translation $\tau : a_i \mapsto a_{i+1 \pmod n}$. We recall that, in this case, any element of H is of the form $\delta_a : i \mapsto a \cdot i \pmod n$ where $\gcd(a, n) = 1$. The following lemma provides a simple way of obtaining $\delta_a(f)$ and $\tau(f)$, for any $f \in C(K, n)$.

Lemma 3.1. *For any $f \in C(K, n)$ and any integers $a, i \ge 0$ such that a and n are relatively prime,*

(i) $\tau^i(f(x)) \equiv x^i \cdot f(x) \pmod{x^n - 1}$,

(ii) $\delta_a(f(x)) \equiv f(x^b) \pmod{x^n - 1}$ *if b is a positive integer such that $ab \equiv 1 \pmod n$.*

Proof. Item (i) follows directly from Example 2.5. For (ii), write $f(x) = \sum_{i=0}^{n-1} a_i x^i$ and let b be any positive integer such that $ab \equiv 1 \pmod n$. Then $\delta_a(f(x)) = \sum_{i=0}^{n-1} a_{i_a} x^i$, where $0 \le i_a \le n-1$ is such that $i_a \equiv ia \pmod n$. Therefore, $i \equiv i_a b \pmod n$ and so $x^i \equiv x^{i_a b} \pmod{x^n - 1}$. In particular,

$$\delta_a(f(x)) \equiv g(x^b) \pmod{x^n - 1},$$

where $g(x) = \sum_{i=0}^{n-1} a_{i_a} x^{i_a} = f(x)$. □

3.1. Proof of Theorem 1.1. Let $W_G(u)$ be the K-vector space spanned by the set $\{\delta(f_u)\}_{\delta \in G}$ and let $a_1, \ldots, a_s$ be a set of positive integers such that H comprises the permutations $\{\delta_{a_j}\}_{1 \le j \le s}$. From previous observations, any element of G can be written uniquely as $\tau^i \delta_{a_j}$, where $0 \le i \le n-1$ and $1 \le j \le s$. Therefore,

$$W_G(u) = \left\{ \sum_{j=1}^{s} \sum_{i=0}^{n-1} c_{i,j} \cdot (\tau^i \delta_{a_j})(f_u(x)) \,|\, c_{i,j} \in K \right\}.$$

Let $b_1, \ldots, b_s$ be positive integers such that $b_i a_i \equiv 1 \pmod n$. From Lemma 3.1, $W_G(u)$ is isomorphic to the K-vector space

$$S_H(u) := \left\{ \sum_{j=1}^{s} g_j(x) \cdot f_u(x^{b_j}) \pmod{x^n - 1} \,|\, g_j \in C(K, n) \right\}.$$

Therefore, from Proposition 2.6, $d_G(u)$ equals the dimension of $S_H(u)$. Since H is a group, the elements a_j comprise a (multiplicative) group modulo n. Moreover, $f(x^a) \equiv f(x^{a'}) \pmod{x^n - 1}$ whenever $a \equiv a' \pmod n$ and so

$$M_{u,H}(x) = \gcd(f_u(x^{b_1}), \ldots, f_u(x^{b_s}), x^n - 1) = \gcd(f_u(x^{a_1}), \ldots, f_u(x^{a_s}), x^n - 1).$$

In addition, since $K[x]$ is a principal domain, we have the isomorphism

$$S_H(u) = \{g(x) \cdot M_{u,H}(x) \pmod{x^n - 1} \,|\, g \in C(k, n)\} \cong C(K, n - \deg(M_{u,H}(x))).$$

In conclusion, $d_G(u) = n - \deg(M_{u,H}(x))$.

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

3.2. Applications of Theorem 1.1. We present some direct consequences of Theorem 1.1.

Definition 3.2. For a subgroup G of S_n and a field K, let $S_{G,K,n} \subseteq \{0, 1, \ldots, n\}$ denote the spectrum of different values of $d_G(u)$, where u runs over K^n.

Let K be a field of characteristic zero and, for each positive integer d, let $\Omega(d)$ be the set of dth primitive roots of unity. We set $\Phi_d(x) = \prod_{\gamma \in \Omega(d)}(x - \gamma)$, the dth cyclotomic polynomial. We observe that, for any $\gamma \in \Omega(d)$,

$$\Phi_d(x) = \prod_{\substack{1 \le j \le d \\ \gcd(j,d)=1}} (x - \gamma^j). \tag{3.1}$$

Thus $\deg(\Phi_d(x)) = \varphi(d)$, where φ is the Euler phi function, and we easily obtain the identity $x^n - 1 = \prod_{d|n} \Phi_d(x)$. If K has characteristic $p > 0$, under the restriction $\gcd(n, p) = 1$, $\Phi_n(x)$ is defined in the same way and the same properties hold. If $n = p^t \cdot n_0$ with $\gcd(n_0, p) = 1$, we have the identity $x^n - 1 = \prod_{d|n_0} \Phi_d(x)^{p^t}$.

Definition 3.3. For positive integers n and r, let $C[n, r] \subseteq \{0, 1, \ldots, nr\}$ be the set of distinct sums of the form $\sum_{d|n} e_d \cdot \varphi(d)$ with $e_d \in \{0, 1, \ldots, r\}$.

Since $\sum_{d|n} \varphi(d) = n$ and $\varphi(1) = 1$,

$$\{0, 1, n-1, n\} \subseteq C[n, 1] \subseteq \{0, 1, \ldots, n\},$$

for any $n \ge 1$. The equality $C[n, 1] = \{0, 1, n - 1, n\}$ occurs exactly when n is a prime number. The other extreme yields the so called φ-practical numbers.

Definition 3.4. A positive integer n is φ-practical if $C[n, 1] = \{0, 1, \ldots, n\}$.

Remark 3.5. The φ-practical numbers have been extensively explored. In particular, if $s(t)$ denotes the number of φ-practical numbers up to t, then $\lim_{t\to\infty} s(t) \cdot \log t/t$ is a positive constant [3]. This shows that the φ-practical numbers are, up to a constant, as frequent as the prime numbers and, in particular, their density in $\mathbb{N}$ is zero.

Lemma 3.6. *Let G, K and n be as in Theorem 1.1. Then $S_{G,K,n} \supseteq C[n, 1]$. If K has characteristic $p > 0$ and $n = p^t \cdot n_0$ with $\gcd(n_0, p) = 1$, then $S_{G,K,n} \supseteq C[n_0, p^t] \supseteq C[n,1]$. In particular, if n is φ-practical, $S_{G,K,n} = \{0, 1, \ldots, n\}$.*

Proof. Let p be the characteristic of K. We split the proof into cases.

Case 1: $p = 0$, or $p > 0$ and $\gcd(n, p) = 1$. In this case, $x^n - 1$ is separable and the equality $x^n - 1 = \prod_{d|n} \Phi_d(x)$ holds over K. Write $G = (\tau, H)$, where H is a subgroup of $\mathbb{Z}_n^*$, and let $a_1, \ldots, a_s$ be a set of positive integers such that H comprises their reductions modulo n. In particular, in the notation of Theorem 1.1, for any $u \in K^n$ we may write

$$M_{H,u}(x) = \gcd(f_u(x^{a_1}), \ldots, f_u(x^{a_s}), x^n - 1) = \prod_{d|n} M_{H,u}^{[d]}(x), \tag{3.2}$$

where $M_{H,u}^{[d]}(x) = \gcd(f_u(x^{a_1}), \ldots, f_u(x^{a_s}), \Phi_d(x))$.

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

We claim that if $\Phi_d(x)$ divides $f_u(x)$, then it divides every polynomial $f_u(x^{a_j})$ and so $M_{H,u}^{[d]}(x) = \Phi_d(x)$. To see this, suppose that $\Phi_d(x)$ divides $f_u(x)$ and let $\gamma \in \overline{K}$ be any root of $\Phi_d(x)$ and j any positive integer with $1 \le j \le s$. Since $\gcd(a_j, n) = 1$ and $\Phi_d(x)$ divides $f_u(x)$, from (3.1), γ^{a_j} is a root of f_u and so γ is a root of $f_u(x^{a_j})$. Since $x^n - 1$ is separable, so is $\Phi_d(x)$. Therefore, $\Phi_d(x)$ divides every $f_u(x^{a_j})$.

For $N = \sum_{d|n} e_d \cdot \varphi(d)$ with $e_d \in \{0, 1\}$, set $f_N(x) = \prod_{d|n} \Phi_d(x)^{1-e_d} = \sum_{i=0}^{n-1} u_i x^i$ in $K[x]$ and $u(N) = (u_0, \ldots, u_{n-1}) \in K^n$. From (3.2) and the previous observations, $M_{H,u(N)}(x) = f_N(x)$ and so, from (1.1),

$$d_G(u(N)) = n - \deg(f_N(x)) = N,$$

since $\sum_{d|n} \varphi(d) = n$.

Case 2. $p > 0$ and $n = p^t \cdot n_0$, where $\gcd(n_0, p) = 1$. The proof that $S_{G,K,n} \supseteq C[n_0, p^t]$ follows similar steps to case 1, using

$$x^n - 1 = \prod_{d|n_0} \Phi_d(x)^{p^t}.$$

We are left to prove the inclusion $C[n_0, p^t] \supseteq C[n, 1]$. Let $N \in C[n, 1]$ and write $N = \sum_{d|n} e_d \cdot \varphi(d)$ with $e_d \in \{0, 1\}$. In particular, we may rewrite

$$N = \sum_{d|n_0} \sum_{i=0}^{t} e_{p^i d} \cdot \varphi(p^i) \cdot \varphi(d) = \sum_{d|n_0} e_d^* \cdot \varphi(d),$$

where $e_d^* = \sum_{i=0}^{t} e_{p^i d} \cdot \varphi(p^i) \le \sum_{i=0}^{t} \varphi(p^i) = p^t$. Therefore, $N \in C[n_0, p^t]$. □

The previous lemma implies $S_{G,K,n} \supseteq C[n, 1]$. More than that, our proof provides a constructive method to produce an element $u \in K^n$ with prescribed dimension $d_G(u) \in C[1, n]$. The following proposition shows that, under some not too restrictive conditions, equation (1.1) can be refined to give the equality $S_{G,K,n} = C[1, n]$.

Theorem 3.7. *Let G, K and n be as in Theorem 1.1. In addition, suppose that K has characteristic p, where $p = 0$ or $p > 0$ and* $\gcd(p, n) = 1$. *Then, for any $u \in K^n$,*

$$d_G(u) = n - \sum_{\substack{d|n \\ \Phi_d(x)|f_u(x)}} \varphi(d), \tag{3.3}$$

in each of the following cases:

(i) *$\Phi_d(x)$ is irreducible over $K[x]$ for any divisor d of n;*
(ii) *$G = \mathbb{G}$.*

In particular, in these cases, $S_{G,K,n} = C[n, 1]$. In additional, in case (i)*,*

$$d_G(u) = n - \deg(\gcd(f_u(x), x^n - 1)) = d_{\mathbb{G}_0}(u),$$

where $\mathbb{G}_0 = \langle \tau \rangle$ is the group generated by the translation $\tau : i \mapsto i + 1 \pmod{n}$.

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

PROOF. Under our hypothesis, $x^n - 1$ is separable and the equality $x^n - 1 = \prod_{d|n} \Phi_d(x)$ holds over K. Write $G = (\tau, H)$ and let $a_1, \ldots, a_s$ be a set of positive integers such that H comprises their reductions modulo n. We are under the conditions of case 1 in Lemma 3.6. In the notation of the lemma, for any $u \in K^n$,

$$M_{H,u}(x) = \prod_{d|n} M_{H,u}^{[d]}(x), \quad \text{where } M_{H,u}^{[d]}(x) = \gcd(f_u(x^{a_1}), \ldots, f_u(x^{a_s}), \Phi_d(x)).$$

Claim. Under the cases (i) or (ii), $M_{H,u}^{[d]}(x) = \Phi_d(x)$ or 1, according as $\Phi_d(x)$ does or does not divide $f_u(x)$.

PROOF OF CLAIM. If $\Phi_d(x)$ divides $f_u(x)$, from the proof of case 1 in Lemma 3.6, we have $M_{H,u}^{[d]}(x) = \Phi_d(x)$. Now, suppose that $f_u(x)$ is not divisible by $\Phi_d(x)$. If $\Phi_d(x)$ is irreducible over $K[x]$, it follows that $\gcd(\Phi_d(x), f_u(x)) = 1$ and so $M_{H,u}^{[d]}(x) = 1$. If $G = \mathbb{G}$, then $H = \mathbb{Z}_n^*$ and so, from (3.1), for any root γ of $\Phi_d(x)$, the set $\{\gamma^a\}_{a\in H}$ contains the roots of $\Phi_d(x)$. In particular, if γ were a root of $f_u(x^a)$ for every $a \in H$, then $f_u(x)$ would be divisible by $\Phi_d(x)$, contrary to our assumption. Therefore, $M_{H,u}^{[d]}(x) = 1$. □

From the claim, $M_{H,u}^{[d]}(x) = \gcd(f_u(x), \Phi_d(x))$. Also, $M_{H,u}(x) = \gcd(f_u(x), x^n - 1)$ from (3.2). Hence (3.3) follows from (1.1). Again, from the claim, $M_{H,u}^{[d]}(x) = 1$ or $\Phi_d(x)$. Since $M_{H,u}(x) = \prod_{d|n} M_{H,u}^{[d]}(x)$ and $\Phi_d(x)$ has degree $\varphi(d)$, from (1.1), it follows that $S_{G,K,n} \subseteq \{n - e \mid e \in C[n, 1]\} = C[n, 1]$. The reverse inclusion $S_{G,K,n} \supseteq C[n, 1]$ follows from Lemma 3.6. □

For any subgroup J of S_n and any subgroup J_0 of J, we have $V_{J_0}(u) \subseteq V_J(u)$ for any $u \in K^n$ and so $d_{J_0}(u) \leq d_J(u)$. In particular, $d_G(u) \geq d_{\mathbb{G}_0}(u)$ for any subgroup G of $\mathbb{G}$ containing $\mathbb{G}_0 = \langle\tau\rangle$ and any $u \in K^n$. By Theorem 3.7, under the conditions of case (i), $d_G(u) = d_{\mathbb{G}_0}(u)$. In other words, the group G does not add any extra information when compared to $\mathbb{G}_0$.

It is well known that $\mathbb{Q}$ admits cyclic Galois extensions of any degree and the cyclotomic polynomials are always irreducible over $\mathbb{Q}$. The following result is straightforward.

COROLLARY 3.8. *Let G be as in Theorem 1.1. Then, for any positive integer n and any $u \in \mathbb{Q}^n$, $d_G(u) = n - \deg(\gcd(f_u(x), x^n - 1))$. In particular, with $S_{G,\mathbb{Q},n}$ as in Definition 3.2,*

$$S_{G,\mathbb{Q},n} = C[n, 1].$$

The next result follows by the same steps as in the proof of Theorem 3.7.

COROLLARY 3.9. *Let G, K and n be as in Theorem 1.1. In addition, suppose that K has characteristic $p > 0$, $n = p^t \cdot n_0$ with $t \geq 1$, and $\gcd(p, n_0) = 1$. If $\Phi_d(x)$ is irreducible over $K[x]$ for each divisor d of n_0 or $G = \mathbb{G}$, for any $u \in K^n$,*

$$d_G(u) = n - \sum_{\substack{d|n_0 \\ \Phi_d(x)|f_u(x)}} \nu(d, u) \cdot \varphi(d), \tag{3.4}$$

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

where $\nu(d,u) \le p^t$ is the greatest positive integer s such that $\Phi_d(x)^s$ divides $f_u(x)$. In particular, $S_{G,K,n} = C[n_0, p^t]$.

For completeness, we comment on the proof of Corollary 1.2. Observe that, for $u = (u_0, \dots, u_{n-1}) \in K^n$, $f_u(x)$ is divisible by $x^n - 1$ if and only if u is the zero vector, $f_u(x)$ is divisible by $x - 1$ if and only if $\sum_{i=0}^{n-1} u_i = f_u(1) = 0$, and $f_u(x)$ is divisible by $(x^n - 1)/(x - 1) = x^{n-1} + \cdots + x + 1$ if and only if $u = (u_0, \dots, u_0)$. Let K, G and n be as in Corollary 1.2. Since n is a prime and $x^{n-1} + \cdots + x + 1$ is irreducible, we observe that K has characteristic p, where $n \ne p$ unless $n = p = 2$. In particular, unless $n = p = 2$, $x^{n-1} + \cdots + x + 1 = \Phi_n(x)$ and Corollary 1.2 follows by the previous observations and (3.3). The case $n = p = 2$ of Corollary 1.2 follows by the previous observations and (3.4).

3.2.1. The finite field case. Let $K = \mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime p. It is well known that, up to isomorphism, there exists a unique extension of $\mathbb{F}_q$ of degree n for any $n \ge 1$. In addition, this extension is a cyclic Galois extension. The following result provides a complete characterisation of the degree distribution in the factorisation of cyclotomic polynomials over $\mathbb{F}_q$.

Lemma 3.10 [2, Theorem 2.47]. *For any positive integer n such that* $\gcd(n, p) = 1$, *let $m := \mathrm{ord}_n q$ be the least positive integer such that $q^m \equiv 1 \pmod n$. Then $\Phi_n(x)$ factors into $\varphi(n)/m$ irreducible polynomials over $\mathbb{F}_q$, each of degree m.*

In particular, $\Phi_d(x)$ is irreducible if and only if $\mathrm{ord}_d q = \varphi(d)$, that is, q is a primitive root modulo d. It is well known that, if d is a power of an odd prime, there exist primitive roots modulo d. In addition, if r is an odd prime and q is a primitive root modulo r^2, then q is a primitive root modulo r^t for any $t \ge 1$. We introduce the Euler phi function for polynomials over finite fields.

Definition 3.11. For any nonzero polynomial $f \in \mathbb{F}_q[x]$, the Euler phi function $E_q(f)$ over $\mathbb{F}_q[x]$ is the number of polynomials $g \in \mathbb{F}_q[x]$ of degree at most $\deg(f(x)) - 1$ such that $\gcd(g(x), f(x)) = 1$. Equivalently,

$$E_q(f) = \left| \left(\frac{\mathbb{F}_q[x]}{(f(x))} \right)^* \right|,$$

where $(f(x))$ is the ideal generated by f over $\mathbb{F}_q[x]$.

From the Chinese remainder theorem, E_q is a multiplicative function. In addition, if $f \in \mathbb{F}_q[x]$ is irreducible of degree d, then $E_q(f) = q^d - 1$. For more details on the Euler phi function for polynomials over finite fields, see [2, Section 3.4].

Theorem 3.12. *Let G be as in Theorem 1.1. Let t be an odd prime and s a positive integer. Suppose that q is a primitive root modulo t^m, where $m = 1$ if $s = 1$, or $m = 2$ if $s \ge 2$. Then, for $n = t^s$ and any $u \in \mathbb{F}_q^{t^s}$,*

$$d_G(u) = t^s - \sum_{\substack{0 \le i \le s \\ \Phi_{t^i}(x) \mid f_u(x)}} \varphi(t^i). \tag{3.5}$$

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

In particular,

$$S_{G,\mathbb{F}_q,t^s} = C[t^s, 1] = \left\{e_0 + (t-1)\cdot\sum_{i=1}^{s} e_i \cdot t^{i-1} \mid e_i \in \{0,1\}\right\},$$

$|S_{G,\mathbb{F}_q,t^s}| = 2^{s+1}$ *and any element* $j \in S_{G,\mathbb{F}_q,t^s}$ *satisfies* $j \equiv 0, 1 \pmod{t-1}$. *Moreover, for any* $r \in S_{G,\mathbb{F}_q,t^s}$ *with*

$$r = e_0 + (t-1)\cdot\sum_{i=1}^{s} e_i \cdot t^{i-1}, \quad e_i \in \{0,1\},$$

the number $N_G(r)$ *of elements* $u \in \mathbb{F}_q^{t^s}$ *such that* $d_G(u) = r$ *is given by*

$$N_G(r) = \prod_{i=0}^{s}(q^{\varphi(t^i)} - 1) = (q-1)^{e_0}\prod_{i=1}^{s}(q^{t^{i-1}(t-1)} - 1)^{e_i}.$$

Proof. We observe that $t \neq p$ and so $x^{t^s} - 1 = \prod_{i=0}^{s}\Phi_{t^i}(x)$. In addition, under our hypothesis, Lemma 3.10 implies that the polynomials $\Phi_{t^i}(x)$ with $0 \le i \le s$ are irreducible. In particular, (3.5) and the equality $S_{G,\mathbb{F}_q,t^s} = C[t^s, 1]$ follow directly from Theorem 3.7. For the equality $|S_{G,\mathbb{F}_q,t^s}| = 2^{s+1}$, we observe that it suffices to prove that the elements of the set

$$\left\{e_0 + (t-1)\cdot\sum_{i=1}^{s} e_i \cdot t^{i-1} \mid e_i \in \{0,1\}\right\},$$

are pairwise distinct. This is easily deduced from the uniqueness of the expansion of a natural number in base t. Finally, let $r = e_0 + (t-1)\cdot\sum_{i=1}^{s} e_i\cdot t^{i-1} \in C[t^s, 1]$, where $e_i \in \{0,1\}$. Since $1 + (t-1)\cdot\sum_{i=1}^{s} t^{i-1} = t^s$,

$$r = t^s - \left[e_0' + (t-1)\cdot\sum_{i=1}^{s} e_i' \cdot t^{i-1}\right] = t^s - \sum_{i=0}^{s} e_i' \cdot \varphi(t^i),$$

where $e_i' = 1 - e_i$. By the previous observations and (3.5), $d_G(u) = r$ if and only if $f_u(x) = g_u(x)\cdot\prod_{i=0}^{s}\Phi_d(x)^{e_i'}$ for some $g_u(x) \in \mathbb{F}_q[x]$ such that $\gcd(g_u(x), x^{t^s} - 1) = 1$. Since $x^{t^s} - 1 = \prod_{i=0}^{s}\Phi_{t^i}(x)$ is separable, if we write $h_r(x) = \prod_{i=0}^{s}\Phi_d(x)^{e_i'}$, the latter is equivalent to $f_u(x) = g_u(x)\cdot h_r(x)$, where $\gcd(g_u(x), H_r(x)) = 1$ and

$$H_r(x) = \frac{x^{t^s} - 1}{h_r(x)} = \prod_{i=0}^{s}\Phi_{t^i}(x)^{e_i}.$$

Since f_u has degree at most $t^s - 1$, g_u has degree at most $t^s - 1 - \deg(h_r(x)) = \deg(H_r(x)) - 1$. We observe that the elements $u \in \mathbb{F}_q^{t^s}$ are in one-to-one correspondence with the polynomials $f \in \mathbb{F}_q[x]$ of degree at most $t^s - 1$ (plus the zero polynomial). From this correspondence, $N_G(r)$ equals the number of polynomials g_u of degree at most $\deg(H_r(x)) - 1$ that are relatively prime with $H_r(x)$, that is, $N_G(r) = E_q(H_r)$.

Table 1. The nonzero values of $N_G(r)$ for $(K, n) = (\mathbb{F}_2, 25)$.

r	0	1	4	5	20	21	24	25
$N_G(r)$	1	1	15	15	$2^{20}-1$	$2^{20}-1$	$15\cdot(2^{20}-1)$	$15\cdot(2^{20}-1)$

Finally, since $H_r(x) = \prod_{i=0}^{s} \Phi_{t^i}(x)^{e_i}$, E_q is multiplicative and each $\Phi_{t^i}(x)$ is irreducible of degree $\varphi(t^i)$,

$$E_q(H_r(x)) = \prod_{i=0}^{s}(q^{\varphi(t^i)} - 1). \qquad \square$$

Example 3.13. Let $q = 2$, $K = \mathbb{F}_2$ and $n = 25 = 5^2$. It is easy to verify that 2 is a primitive root modulo 25. For G as in Theorem 1.1, $S_{G,\mathbb{F}_2,25} = \{0, 1, 4, 5, 20, 21, 24, 25\}$. Table 1 shows the nonzero values of $N_G(r)$ for $r \in S_{G,\mathbb{F}_2,25}$.

4. The dihedral action and the reciprocal of a polynomial

In this section we consider the natural action of the *dihedral group* $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ over K^n. There is a natural embedding D_n into S_n as follows: $D_n = \langle \tau, \eta\rangle$, where $\tau : i \mapsto i + 1 \pmod n$ is the translation and $\eta : i \mapsto n - i \pmod n$ is the reflection. Geometrically, η can be viewed as the reflection of K^n with respect to the variety V_n determined by the equations $x_i = x_{n-i}$ with $1 \le i \le n/2$. Since $n - i \equiv (n - 1)i \pmod n$, Theorem 1.1 implies that, for any $u = (u_0, \dots, u_{n-1}) \in \mathbb{F}_q^n$,

$$d_{D_n}(u) = n - \deg(\gcd(f_u(x), f_u(x^{n-1}), x^n - 1)),$$

where $f_u(x) = \sum_{i=0}^{n-1} u_i x^i$. For a nonzero polynomial $f(x) = \sum_{i=0}^{m} a_i x^i$ in $K[x]$ of degree m, the *reciprocal* of f is the polynomial $f^*(x) = x^m f(1/x) = \sum_{i=0}^{m} a_{m-i} x^i$. The following result is straightforward.

Lemma 4.1. *For a nonzero polynomial $f \in K[x]$ and a nonzero element α in the algebraic closure of K, α is a root of f with multiplicity j if and only if $1/\alpha$ is a root of its reciprocal polynomial f^* with multiplicity j.*

Lemma 4.2. *If $u = (u_0, \dots, u_{n-1}) \in K^n$ is not the zero vector, write*

$$f_u(x) = \sum_{i=0}^{n-1} u_i x^i = g_u(x) \cdot h_u(x),$$

where $h_u(x)$ is relatively prime to $x^n - 1$. Then

$$d_{D_n}(u) = n - d_u,$$

where d_u is the degree of $\gcd(f_u(x), f_u^*(x), x^n - 1) = \gcd(g_u(x), g_u^*(x), x^n - 1)$.

https://doi.org/10.1017/S0004972719000340 Published online by Cambridge University Press

Proof. Let α be any root of $M_u(x) = \gcd(f_u(x), f_u(x^{n-1}), x^n - 1)$. In particular, $\alpha \neq 0$ is a root of $g_u(x)$. We observe that $\alpha^{n-1} = 1/\alpha$ and so $f_u(1/\alpha) = 0$, that is, $f_u^*(\alpha) = 0$. Since $1/\alpha$ is also a root of $x^n - 1$, it follows that $1/\alpha$ is not a root of $h_u(x)$. In conclusion, $\alpha^n - 1 = g_u(\alpha) = g_u(1/\alpha) = 0$. From Lemma 4.1, the latter occurs if and only if $g_u(\alpha) = g_u^*(\alpha) = 0$. Since g_u divides f_u (and g_u^* divides f_u^*),

$$M_u(x) = \gcd(f_u(x), f_u^*(x), x^n - 1) = \gcd(g_u(x), g_u^*(x), x^n - 1),$$

and the result follows. □

From the previous lemma, we can obtain information on the value of $d_{D_n}(u)$ without even computing the greatest common divisor of polynomials. This is exemplified in the following corollary.

Corollary 4.3. *Let n be odd such that $x^n - 1$ has only simple roots over the algebraic closure of K. Then, for $u \in K^n$, we have $\sum_{i=0}^{n-1} u_i = 0$ if and only if $d_{D_n}(u)$ is even.*

Proof. Since n is odd, 1 is the only common root of the polynomials $x^n - 1$ and $x^2 - 1$. In particular, whenever $f_u(x) = \sum_{i=0}^{n} u_i x^i$ and f_u^* have a common root α of $x^n - 1$, $1/\alpha$ is also a common root and such elements are distinct if $\alpha \neq 1$. In other words, if we write $f_u(x) = \sum_{i=0}^{n-1} u_i x^i = g_u(x) \cdot h_u(x)$, where $h_u(x)$ is relatively prime to $x^n - 1$, the common roots of $g_u(x)$ and $x^n - 1$ come in pairs whenever they are distinct from $1 \in K$. From the hypothesis, the polynomial $x^n - 1$ has only simple roots. In particular, if we set $M_u(x) = \gcd(g_u(x), g_u^*(x), x^n - 1)$, $M_u(x)$ has odd degree if and only if it is divisible by $x - 1$. The latter is equivalent to $f_u(1) = 0$, that is, $\sum_{i=0}^{n-1} u_i = 0$. Since n is odd, from Lemma 4.2, $M_u(x)$ has odd degree if and only if $d_{D_n}(u)$ is even. □

References

[1] E. Artin, *Galois Theory*, Notre Dame Mathematical Lectures, 2 (University of Notre Dame, Notre Dame, IN, 1942).

[2] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications* (Cambridge University Press, New York, 1986).

[3] C. Pomerance, L. Thompson and A. Weingartner, 'On integers n for which $x^n - 1$ has a divisor of every degree', *Acta Arith.* **175** (2016), 225–243.

LUCAS REIS, Universidade de São Paulo,
Instituto de Ciências Matemáticas e de Computação,
São Carlos, SP 13560-970, Brazil
e-mail: lucasreismat@gmail.com