Bull. Aust. Math. Soc. **102** (2020), 365–373
doi:10.1017/S000497272000009X

ON SEMIGROUP ORBITS OF POLYNOMIALS AND MULTIPLICATIVE ORDERS

JORGE MELLO

(Received 19 November 2019; accepted 16 December 2019; first published online 20 February 2020)

Abstract

We show, under some natural restrictions, that some semigroup orbits of polynomials cannot contain too many elements of small multiplicative order modulo a large prime p, extending previous work of Shparlinski ['Multiplicative orders in orbits of polynomials over finite fields', *Glasg. Math. J.* **60**(2) (2018), 487–493].

2010 *Mathematics subject classification*: primary 11D45; secondary 14G15, 37P55.

Keywords and phrases: arithmetic dynamics, polynomial mappings, semigroup orbits.

1. Introduction

Let K be a field and $\overline{K}$ its algebraic closure. Let $\mathcal{F} = \{\phi_1, \dots, \phi_k\} \subset K[X]$ be a set of polynomials of degree at least 2. For $x \in K$, let

$$\mathcal{O}_{\mathcal{F}}(x) = \{\phi_{i_n} \circ \cdots \circ \phi_{i_1}(x) : n \in \mathbb{N}, i_j = 1, \dots, k\} \tag{1.1}$$

denote the forward orbit of P under $\mathcal{F}$.

For a prime p and an integer $s \geq 1$, let $\mathbb{F}_{p^s}$ denote the finite field of p^s elements. For $w \in \mathbb{F}_{p^s}$ and $\phi_1, \dots, \phi_k$ defined over $\mathbb{F}_{p^s}$,

$$T(w) := \#\mathcal{O}_{\mathcal{F}}(w) \leq p^s.$$

For $u \in \overline{\mathbb{F}}_p^*$, the multiplicative order $\tau(u)$ is the smallest integer $l \geq 1$ such that $u^l = 1$. When $k = 1$ and $\epsilon > 0$ is arbitrary, Shparlinski [5] obtained the bound

$$\#\{n \leq N - 1 : \tau(f^{(n)}(x)) \leq t\} = O(\max\{N^{1/2}, N/\log\log p\}),$$

for $x \in \overline{\mathbb{F}}_p$, p prime and $t \leq (\log p)^{1/2-\epsilon}$, provided f is not linearly conjugate to a monomial nor to a Chebyshev polynomial.

We seek to generalise results of this sort when the dynamical systems are generated as semigroups under composition by several maps ϕ_i which are not linearly conjugate

For this research, the author was supported by the Australian Research Council Grant DP180100201.

to monomials or to Chebyshev polynomials. Let $\mathcal{F}_n = \{\phi_{i_n} \circ \cdots \circ \phi_{i_1} : 1 \le i_j \le k\}$ denote the n-level set. Let $\epsilon > 0$ and suppose that $h \ge 3l$ are integers such that

$$\#\{v \in \overline{\mathbb{F}}_p : \tau(v) \le t, v = f(u), f \in \mathcal{F}_n, n \le N\} \ge B(k, h)$$

for each N, where $B(k, h)$ is the size of the complete k-tree of depth $h - 1$. We prove, among other results, that

$$\#\{v \in \overline{\mathbb{F}}_p : \tau(v) \le t, v = f(u), f \in \mathcal{F}_n, n \le N\} \ll_{l,\mathcal{F}} \max\left\{\frac{B(k,h)^{l+1}}{h}, \frac{B(k,h)^{l+1}}{\log\log p}\right\},$$

for all $x \in \overline{\mathbb{F}}_p$, p prime and $t \le (\log p)^{1/2-\epsilon}$. That is, if the number of orbit points of iteration order at most N and multiplicative order at most t is bigger than $B(k, h)$, then this number is bounded above in terms of $B(k, h)$ and the characteristic of the field. We use recent results of Ostafe and Young [4] about the finiteness of cyclotomic algebraic points that are preperiodic for $\mathcal{F}$ and that fall on the set of roots of unity, and results from graph theory due to Mérai and Shparlinski [2].

Sections 2, 3 and 5 are devoted to preliminary notation and results. Section 4 contains results for points in orbits generated by sequences of polynomials from the initial set of polynomials and Section 6 contains the result for the full semigroup orbit.

2. Preliminary notation

For K a number field and $x \in K$, the naive logarithmic height $h(x)$ is given by

$$\sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log(\max\{1, |x|_v\}),$$

where M_K is the set of places of K and $|\cdot|_v$ denotes the corresponding absolute value on K for each $v \in M_K$. Let M_K^∞ be the set of archimedean (infinite) places of K and M_K^0 the set of nonarchimedean (finite) places of K. For $v \in M_K^0$, the restriction of $|\cdot|_v$ to $\mathbb{Q}$ gives the usual v-adic absolute value on $\mathbb{Q}$. We write K_v for the completion of K with respect to $|\cdot|_v$ and $\mathbb{C}_v$ for the completion of an algebraic closure of K_v. To simplify notation, we write $d_v = [K_v : \mathbb{Q}_v]/[K : \mathbb{Q}]$.

For an arbitrary field K, let $\mathcal{F} = \{\phi_1, \ldots, \phi_k\} \subset K[X]$ be a dynamical system of polynomials of degree at least 2. For $x \in K$, let $O_{\mathcal{F}}(x)$ denote the forward orbit of P under $\mathcal{F}$ as in (1.1).

Set $J = \{1, \ldots, k\}$ and $W = \prod_{i=1}^\infty J$ (an infinite product of countably many copies of J) and let $\Phi_w := (\phi_{w_j})_{j=1}^\infty$ be a sequence of polynomials from $\mathcal{F}$ for $w = (w_j)_{j=1}^\infty \in W$. In this situation,

$$\Phi_w^{(n)} = \phi_{w_n} \circ \cdots \circ \phi_{w_1} \quad \text{with } \Phi_w^{(0)} = \text{ Id and } \mathcal{F}_n := \{\Phi_w^{(n)} : w \in W\}.$$

That is, we consider sequences of polynomials $\Phi = (\phi_{i_j})_{j=1}^\infty \in \prod_{i=1}^\infty \mathcal{F}$ and, for $x \in \overline{K}$, we write $\Phi^{(n)}(x) := \phi_{i_n}(\phi_{i_{n-1}}(\ldots(\phi_{i_1}(x)))$. The set

$$O_\Phi(x) := \{x, \Phi^{(1)}(x), \Phi^{(2)}(x), \Phi^{(3)}(x), \ldots\}$$

https://doi.org/10.1017/S000497272000009X Published online by Cambridge University Press

is the forward orbit of x under Φ. The point x is called Φ-preperiodic if $\mathcal{O}_\Phi(x)$ is finite. and preperiodic for $\mathcal{F}$ if $\mathcal{O}_{\mathcal{F}}(x)$ is finite.

We let S be the *shift map* which sends $\Psi = (\psi_i)_{i=1}^\infty$ to $S(\Psi) = (\psi_{i+1})_{i=1}^\infty$.

For $\mathcal{S} \subset K$ and an integer $N \geq 1$, we denote by $T_{x,\Phi}(N, \mathcal{S})$ the number of $n \leq N$ with $\Phi^{(n)}(w) \in \mathcal{S}$, that is,

$$T_{x,\Phi}(N, \mathcal{S}) = \#\{n \leq N : \Phi^{(n)}(x) \in \mathcal{S}\}.$$

For $f = \sum_{i=0}^d a_i X^i \in \overline{\mathbb{Q}}[X]$ and K a number field containing all the coefficients of f, the Weil height of f is

$$h(f) = \sum_{v \in M_K} d_v \log(\max_i |a_i|_v).$$

For the system of polynomials $\mathcal{F} = \{\phi_1, \dots \phi_k\}$, we write $h(\mathcal{F}) = \max_i h(\phi_i)$. We will use the following bound for the Weil height.

Proposition 2.1 [1, Proposition 3.3]. *Let $\mathcal{F} = \{\phi_1, \dots, \phi_k\}$ be a finite set of polynomials over a number field K with $\deg \phi_i = d_i \geq 2$, and $d := \max_i d_i$. Then, for all $n \geq 1$ and $\phi \in \mathcal{F}_n$,*

$$h(\phi) \leq \Big(\frac{d^n - 1}{d - 1}\Big) h(\mathcal{F}) + d^2 \Big(\frac{d^{n-1} - 1}{d - 1}\Big) \log 8 = O(d^n(h(\mathcal{F}) + 1)).$$

3. Preliminary results

We will make use of the following combinatorial result.

Lemma 3.1 [3, Lemma 4.8]. *Let $2 \leq T < N/2$. For any sequence*

$$0 \leq n_1 < \cdots < n_T \leq N,$$

there exists $r \leq 2N/T$ such that $n_{i+1} - n_i = r$ for at least $T(T-1)/4N$ values of $i \in \{1, \dots, T-1\}$.

The following result for general fields is a direct application of Lemma 3.1.

Proposition 3.2. *Let K be an arbitrary field, $x \in K$ and $\mathcal{S} \subset K$ an arbitrary subset of K. Suppose that there exist a real number $\tau \in (0, 1/2)$ and a sequence Φ of polynomials contained in $\mathcal{F} = \{\phi_1, \dots, \phi_k\} \subset K[X]$ such that*

$$T_{x,\Phi}(N, \mathcal{S}) = \tau N \geq 2.$$

Then there exists an integer $t \leq 2\tau^{-1}$ such that

$$\#\{(u, v) \in \mathcal{S}^2 : (S^n\Phi)^t(u) = v \text{ for some } n\} \geq \frac{\tau^2 N}{8}.$$

Proof. Letting $T := T_{x,\Phi}(N, \mathcal{S})$, we consider all the values

$$1 \leq n_1 < \cdots < n_T \leq N$$

https://doi.org/10.1017/S000497272000009X Published online by Cambridge University Press

such that $\Phi^{(n_i)}(x) \in \mathcal{S}$, $i = 1, \dots, T-1$. From Lemma 3.1, there exists $t \le 2\tau^{-1}$ such that the number of $i = 1, \dots, T-1$ with $n_{i+1} - n_i = t$ is at least

$$\frac{T(T-1)}{4N} = \frac{T^2}{4}\Big(1 - \frac{1}{T}\Big) = \frac{\tau^2 N}{4}\Big(1 - \frac{1}{T}\Big) \ge \frac{\tau^2 N}{8}.$$

Moreover, if $\mathcal{J} := \{1 \le j \le T-1 : n_{j+1} - n_j = t\}$, then

$$\Phi^{(n_j)}(x) \in \mathcal{S} \quad \text{and} \quad \Phi^{(n_{j+1})}(x) = (S^{n_j}\Phi)^t(\Phi^{(n_j)}(x)) \in \mathcal{S} \quad \text{for each } j \in \mathcal{J}.$$

Consequently,

$$\#\{(u, v) \in \mathcal{S}^2 : (S^n\Phi)^t(u) = v \text{ for some } n\} \ge \frac{\tau^2 N}{8}. \qquad \square$$

4. Multiplicative orders in finite fields

In this section we consider $\mathcal{F} = \{\phi_1, \dots, \phi_k\} \subset \mathbb{Z}[X]$. We also use $\mathcal{F}$ to denote the set of reductions $\phi_1, \dots, \phi_k$ mod p. For a sequence Ψ of terms in $\mathcal{F}$, we write

$$M_{w,\Psi}(t, N) = \#\{n \le N-1 : \tau(\Psi^{(n)}(w)) \le t\},$$

where τ is the multiplicative order in $\overline{\mathbb{F}}_p^*$. We use $\mathbb{U}$ to denote the set of all roots of unity in $\mathbb{C}$ and Φ_s to denote the cyclotomic polynomial of order s. The resultant of two polynomials $F, G \in \mathbb{Z}[X]$ is denoted by $\mathrm{Res}(F, G)$. The next lemma is well known.

Lemma 4.1 [5, Lemma 2.6]. *For any integers $r, s \ge 1$ and $F \in \mathbb{Z}[X]$,*

$$\mathrm{Res}(\Phi_r, \Phi_s(F)) = \exp(O(rs(h(F) + \deg F))).$$

We now formulate special cases of results due to Ostafe and Young [4]. For these and for all the following results, we say that a polynomial in $\mathbb{Z}[X]$ is *nonspecial* if it is not linearly conjugate to any monomial or any Chebyshev polynomial.

Lemma 4.2. *Let $\mathcal{F} = \{\phi_1, \dots, \phi_k\} \in \mathbb{Z}[X]$ be a set of nonspecial polynomials of respective degrees $d_i \ge 2$. Then $\phi_i(\mathbb{Q}(\mathbb{U}))$ is finite for each i and so is the set of $u \in \mathbb{Q}(\mathbb{U})$ such that $\mathcal{O}_{\mathcal{F}}(u) \cap \mathbb{U} \ne \emptyset$.*

Proof. Use [3, Corollary 2.2] and [4, Theorem 1.4]. $\square$

Lemma 4.3 [4, Theorem 1.7]. *Under the conditions of the previous lemma,*

$$\{\alpha \in \mathbb{Q}(\mathbb{U}) : \phi_{i_s} \circ \cdots \circ \phi_{i_1}(\alpha) \in \mathcal{F}_l(\phi_{i_s} \circ \cdots \circ \phi_{i_1}(\alpha)), s \ge 0, l \ge 1\}$$

is finite.

Next we aim to bound the number of elements of bounded order in an orbit.

Theorem 4.4. *Let $\mathcal{F} = \{\phi_1, \dots, \phi_k\} \in \mathbb{Z}[X]$ be a set of nonspecial polynomials of respective degrees $d_i \ge 2$ and let $d = \max_i d_i$. Take any fixed $\epsilon > 0$.*

https://doi.org/10.1017/S000497272000009X Published online by Cambridge University Press

(i) *For any prime p and $t \le (\log p)^{1/2-\epsilon}$ and for all initial values $w \in \overline{\mathbb{F}}_p$,*

$$\sup_{\Psi \text{ sequence in } \mathcal{F}} M_{w,\Psi}(t, N) = O(\max\{N^{1/2}, N/\log\log p\}).$$

(ii) *Let Ψ be a sequence of terms in $\mathcal{F}$. Then, for any sufficiently large $P \ge 1$ and $t \le P^{1/2-\epsilon}$, for almost all primes $p \le P$ and for all initial values $w \in \overline{\mathbb{F}}_p$,*

$$M_{w,\Psi}(t, N) = O(\max\{N^{1/2}, N/\log p\}).$$

Proof. For $w \in \overline{\mathbb{F}}_p$ and Ψ a sequence of terms in $\mathcal{F}$, write

$$M_{w,\Psi}(t, N) := \rho_\Psi N.$$

Then there are at least $\rho_\Psi N$ values of $n < N$ with $\Phi_l(\Psi^{(n)}(w)) = 0$ for some positive integer $l \le t$. By Proposition 3.2, there is some positive integer $m_\Psi \le 2\rho_\Psi^{-1}$ such that, for at least $\rho_\Psi^2 N/8$ values $u \in \overline{\mathbb{F}}_p^*$,

$$\Phi_s(u) = \Phi_l(\gamma(u)) = 0,$$

for some pair $(s, l) \in [1, t]^2$ and $\gamma = (S^n\Psi)^{(m_\Psi)} \in \mathcal{F}_{m_\Psi}$. Denote by $R_{s,l,m_\Psi,\gamma}$ the resultant of the polynomials $\Phi_s(X)$ and $\Phi_l(\gamma(X))$. By Lemma 4.2, there are only finitely many values of m_Ψ for which $R_{s,l,m_\Psi,\gamma} = 0$ is possible for some s, l and γ. Then there are at most c_1 values of $u \in \overline{\mathbb{F}}_p$ giving solutions of $R_{s,l,m_\Psi,\gamma} = 0$, where c_1 does not depend on Ψ but only on $\mathcal{F}$. If $\rho_\Psi^2 N/8 > c_1$, there exists (s, l, m_Ψ, γ) such that $p \mid R_{s,l,m_\Psi,\gamma} \ne 0$.

If this is the case, then $\rho_\Psi > \sqrt{8c_1/N}$. Using Lemma 4.1 and Proposition 2.1 with $d = \max_i d_i$,

$$\log |R_{s,l,m_\Psi,\gamma}| = O(sld^{m_\Psi}) = O(t^2 d^{2\rho_\Psi{}^{-1}}).$$

This does not depend on p, or on the initial values of Ψ from which ρ_Ψ was derived, and so $\log p = O(t^2 d^{2\rho_\Psi{}^{-1}})$. But $t \le (\log p)^{1/2-\epsilon}$, so $(\log p)^{2\epsilon} \le t^{-2} \log p = O(d^{2\rho_\Psi{}^{-1}})$ and therefore $\rho_\Psi \le c_2(\log\log p)^{-1}$. Taking

$$\rho_\Psi = \max\{3\sqrt{c_1/N}, 2c_2(\log\log p)^{-1}\},$$

where the constant c_2 depends only on $\mathcal{F}$, induces a contradiction. This proves (i).

For (ii), consider $\Omega(R_{s,l,m_\Psi,\gamma})$, where $\Omega(r)$ denotes the number of distinct prime divisors of an integer $r \ne 0$. If $R_{s,l,m_\Psi,\gamma} \ne 0$, then

$$\Omega(R_{s,l,m_\Psi,\gamma}) \le 2\log |R_{s,l,m_\Psi,\gamma}| = O(t^2 d^{2\rho_\Psi{}^{-1}}) = O(P^{1-2\epsilon} d^{2\rho_\Psi{}^{-1}}).$$

This does not depend on p, or on the initial values of Ψ from which ρ_Ψ was derived. If $\rho_\Psi \ge (2\log d)/(\epsilon \log P)$, it follows that $\Omega(R_{s,l,m_\Psi,\gamma}) = o(P/\log P)$. Consequently, in this case, $\max_\Phi \rho_\Phi \le O(1/\log p)$ for all but $o(P/\log P)$ primes. □

Corollary 4.5. *Let $\mathcal{F} = \{\phi_1, \ldots, \phi_k\} \in \mathbb{Z}[X]$ be a set of nonspecial polynomials of respective degrees $d_i \ge 2$ and $d = \max_i d_i$. Then, for any fixed $\epsilon > 0$, for any prime p and $t \le (\log p)^{1/2-\epsilon}$ and for all initial values $w \in \overline{\mathbb{F}}_p$,*

$$\#\{u \in \overline{\mathbb{F}}_p : u = f(w), \tau(u) \le t, f \in \mathcal{F}_n, n \le N - 1\} = O(\max\{N^{1/2}k^N, Nk^N/\log\log p\}).$$

https://doi.org/10.1017/S000497272000009X Published online by Cambridge University Press

Proof. The set $\mathcal{F}_N$ contains k^N polynomials. For each $f \in \mathcal{F}_N$, we can choose a sequence Φ of terms in $\mathcal{F}$ such that $\Phi^{(N)} = f$, obtaining k^N sequences representing the elements of $\mathcal{F}_N$. For each such sequence Φ, by Theorem 4.4,

$$M_{w,\Psi}(t, N) = O(\max\{N^{1/2}, N/\log\log p\})$$

uniformly for any Φ, or in other words, for each path in the N-tree $\mathcal{F}_N$. Since there are k^N paths (polynomials and sequences) in the n-tree $\mathcal{F}_N$, this yields

$$\#\{u \in \overline{\mathbb{F}}_p : u = f(w), \tau(u) \le t, f \in \mathcal{F}_n, n \le N-1\} = O(\max\{N^{1/2}k^N, Nk^N/\log\,\log p\}).$$

$\square$

Theorem 4.6. *Let $\mathcal{F} = \{\phi_1, \ldots, \phi_k\} \in \mathbb{Z}[X]$ be a set of nonspecial polynomials of respective degrees $d_i \ge 2$ and $d = \max_i d_i$. Let $s(w)$ be the minimum number of sequences Ψ_i of terms in $\mathcal{F}$ such that $\mathcal{O}_{\mathcal{F}}(w) = \mathcal{O}_{\Psi_1}(w) \cup \cdots \cup \mathcal{O}_{\Psi_{s(w)}}(w)$. Then, for any prime p and for all but $O(1)$ initial values $w \in \overline{\mathbb{F}}_p$,*

$$d^{T(w)}\tau(w)^{s(w)} \gg (\log p)^{s(w)}.$$

Proof. For a sequence Ψ of functions from $\mathcal{F}$ and $w \in \overline{\mathbb{F}}_p$, we set $T_\Psi(w) := \#\mathcal{O}_\Psi(w)$.

There are integers m_Ψ, l_Ψ, n with $T(w) \ge T_\Psi(w) \ge m_\Psi > l_\Psi \ge 0$ and $n = \tau(w)$, so that $\Psi^{(m_\Psi)}(w) = \Psi^{(l_\Psi)}(w)$ and $\Phi_n(w) = 0$. Taking $Q_{m_\Psi,l_\Psi,n}$ as the resultant of the polynomials $\Psi^{(m_\Psi)}(X) - \Psi^{(l_\Psi)}(X)$ and $\Phi_n(X)$, it follows that

$$p \mid Q_{m_\Psi,l_\Psi,n}.$$

If $|Q_{m_\Psi,l_\Psi,n}| < p$, then $Q_{m_\Psi,l_\Psi,n} = 0$ and thus the polynomials $\Psi^{(m_\Psi)}(X) - \Psi^{(l_\Psi)}(X)$ and $\Phi_n(X)$ have a common root in $\mathbb{C}$. By Lemma 4.3, there are only $O(1)$ possible values of n where this can happen, and therefore only finitely many possibilities for $w \in \overline{\mathbb{F}}_p$.

Now, note that $d^{m_\Psi} n \le d^{T_\Psi(w)}\tau(w)$. By Lemma 4.1 with $r = n$, $s = 1$,

$$|Q_{m_\Psi,l_\Psi,n}| = \exp(O(d^{m_\Psi} n)) = \exp(O(d^{T_\Psi(w)}\tau(w))),$$

where O does not depend on the initial values of Ψ from which m_Ψ was derived. If c_0 is chosen small enough not depending on Ψ, then $d^{T_\Psi(w)}\tau(w) \le c_0 \log p$ implies $|Q_{m_\Psi,l_\Psi,n}| < p$, and then $d^{T_\Psi(w)}\tau(w) \gg \log p$ for all but $O(1)$ values $w \in \overline{\mathbb{F}}_p$, where none of the implied constants depend on Ψ.

Let $s(w)$ be the minimum number of sequences Ψ_i of terms in $\mathcal{F}$ such that $\mathcal{O}_{\mathcal{F}}(w) = \mathcal{O}_{\Psi_1}(w) \cup \cdots \cup \mathcal{O}_{\Psi_{s(w)}}(w)$. Then

$$d^{T(w)}\tau(w)^{s(w)} \ge d^{T_{\Psi_1}(w)}\tau(w) \cdots d^{T_{\Psi_{s(w)}}(w)}\tau(w) \gg (\log p)^{s(w)}$$

for all but $O(1)$ values of $w \in \overline{\mathbb{F}}_p$. $\square$

https://doi.org/10.1017/S000497272000009X Published online by Cambridge University Press

5. A graph theory result

Here we present a graph theory result of Mérai and Shparlinski [2] that will be used in our next result.

Let $\mathcal{H}$ be a directed graph, possibly with multiple edges. Let $\mathcal{V}(\mathcal{H})$ be the set of vertices of $\mathcal{H}$. For $u, v \in \mathcal{V}(\mathcal{H})$, let $d(u, v)$ be the distance from u to v, that is, the length of a shortest (directed) path from u to v. Assume that all the vertices have out-degree $k \geq 1$ and label the edges from each vertex by $\{1, \ldots, k\}$.

For a word $\omega \in \{1, \ldots, k\}^*$ over the alphabet $\{1, \ldots, k\}$ and a vertex $u \in \mathcal{V}(\mathcal{H})$, let $\omega(u) \in \mathcal{V}(\mathcal{H})$ be the end point of the walk starting from u and following the edges according to ω.

Fix $u \in \mathcal{V}(\mathcal{H})$ and a subset $\mathcal{A} \subset \mathcal{V}(\mathcal{H})$. Then, for words $\omega_1, \ldots, \omega_l$, put

$$\begin{aligned}L_N(u, \mathcal{A}; \omega_1, \ldots, \omega_l) = \#\{v \in \mathcal{V}(\mathcal{H}) : d(u, v) \leq N,\\ d(u, \omega_i(v)) \leq N, \omega_i(v) \in \mathcal{A}, i = 1, \ldots, l\}.\end{aligned}$$

For $k, h \geq 1$, let $B(k, h)$ denote the size of the complete k-tree of depth $h - 1$, that is,

$$B(k, h) = \begin{cases} h & \text{if } k = 1, \\ \dfrac{k^h - 1}{k - 1} & \text{otherwise.} \end{cases}$$

Lemma 5.1. *Let $u \in \mathcal{V}(\mathcal{H})$ and $h, l \geq 1$ be fixed. If $\mathcal{A} \subset \mathcal{V}(\mathcal{H})$ is a subset of vertices with*

$$\#\{v \in \mathcal{A} : d(u, v) \leq N\} \geq \max\Big\{3B(k, h), \frac{3l}{h}\#\{v \in \mathcal{V}(\mathcal{H}) : d(u, v) \leq N\}\Big\},$$

then there exist words $\omega_1, \ldots, \omega_l \in \{1, \ldots, k\}^*$ of length at most h such that

$$L_N(u, \mathcal{A}; \omega_1, \ldots, \omega_l) \gg \frac{h}{B(k, h)^{l+1}}\#\{v \in \mathcal{V}(\mathcal{H}) : d(u, v) \leq N\},$$

where the implied constant depends only on l.

6. Another semigroup result about multiplicative orders

Theorem 6.1. *Let $\mathcal{F} = \{\phi_1, \ldots, \phi_k\} \in \mathbb{Z}[X]$ be a set of nonspecial polynomials of respective degrees $d_i \geq 2$ and $d = \max_i d_i$. Let $h, l \geq 1$ be integers such that $h \geq 3l$ and $\#\{v \in \overline{\mathbb{F}}_p : \tau(v) \leq t, v = f(u), f \in \mathcal{F}_n, n \leq N\} \geq 3B(k, h)$. Take any fixed $\epsilon > 0$.*

(i) *For any prime p and $t \leq (\log p)^{1/2-\epsilon}$ and for all initial values $u \in \overline{\mathbb{F}}_p$,*

$$\#\{v \in \overline{\mathbb{F}}_p : v = f(u), \tau(u) \leq t, f \in \mathcal{F}_n, n \leq N\} \ll_{l,\mathcal{F}} \max\Big\{\frac{B(k, h)^{l+1}}{h}, \frac{B(k, h)^{l+1}}{\log\log p}\Big\}.$$

(ii) *For any sufficiently large $P \geq 1$ and $t \leq P^{1/2-\epsilon}$, for almost all primes $p \leq P$ and for all initial values $u \in \overline{\mathbb{F}}_p$,*

$$\#\{v \in \overline{\mathbb{F}}_p : v = f(u), \tau(u) \leq t, f \in \mathcal{F}_n, n \leq N\} \ll_{l,\mathcal{F}} \max\Big\{\frac{B(k, h)^{l+1}}{h}, \frac{B(k, h)^{l+1}}{\log p}\Big\}.$$

https://doi.org/10.1017/S000497272000009X Published online by Cambridge University Press

PROOF. Set

$$\Gamma := \{x \in \overline{\mathbb{F}}_p^* : \tau(y) \le t\}.$$

We consider the directed graph with the elements of Γ as vertices and edges $(x, \phi_i(x))$ for $i = 1, \ldots, k$ and $x \in \Gamma$. In the notation of Section 5 and Lemma 5.1, we let Γ take the place of $\mathcal{H}$ and $\mathcal{A}$. By hypothesis, $l \le h/3$ and $\#\{v \in \Gamma : d(u, v) \le N\} \ge 3B(k, h)$. From Lemma 5.1, there exist words $\omega_1, \ldots, \omega_l \in \{1, \ldots, k\}^*$ of length at most h and therefore degree at most d^h, such that

$$L_N(u, \Gamma; \omega_1, \ldots, \omega_l) \ge c_1 \frac{h}{B(k, h)^{l+1}} \#\{v \in \mathcal{V}(\Gamma) : d(u, v) \le N\}, \tag{6.1}$$

with c_1 a positive constant depending only on l.

If $v \in L_N(u, \Gamma; \omega_1, \ldots, \omega_l)$, then $\{v, \omega_i(v)\} \subset \Gamma$ for each i. This means that, for a given $i = 1, \ldots, l$,

$$\Phi_r(v) = \Phi_s(w_i(v)) = 0$$

for some $r, s \in [1, t]^2$. Denote by R_{r,s,ω_i} the resultant of the polynomials $\Phi_r(X)$ and $\Phi_s(\omega_i(X))$. By Lemma 4.2, there are at most c_2 values of $v \in \overline{\mathbb{F}}_p$ which are solutions of $R_{r,s,\omega_i} = 0$, and therefore $c_2 \ge L_N(u, \Gamma; \omega_1, \ldots, \omega_l)$. If

$$\#\{v \in \mathcal{V}(\Gamma) : d(u, v) \le N\} > \frac{c_2 B(k, h)^{l+1}}{c_1 h}, \tag{6.2}$$

there exists a triple (r, s, ω_i) such that $p \mid R_{r,s,\omega_i} \ne 0$. In this case, using Lemma 4.1 and Proposition 2.1 with $d = \max_i d_i$,

$$\log |R_{r,s,\omega_i}| = O(rsd^h) = O(t^2 d^h),$$

where the implied constants do not depend on p. Thus, $\log p = O(t^2 d^h)$. By hypothesis, $t \le (\log p)^{1/2-\epsilon}$, and so it follows that $(\log p)^{2\epsilon} \le t^{-2} \log p = O(d^h)$, and therefore $h^{-1} \le c_3 (\log\log p)^{-1}$. By (6.1),

$$\#\{v \in \mathcal{V}(\Gamma) : d(u, v) \le N\} \le \frac{c_2 B(k, h)^{l+1}}{c_1 h} \le \frac{c_2 c_3 B(k, h)^{l+1}}{c_1 \log\log p}. \tag{6.3}$$

Consequently, if

$$\#\{v \in \mathcal{V}(\Gamma) : d(u, v) \le N\} \ge \max\left\{\frac{2c_2 B(k, h)^{l+1}}{c_1 h}, 2\frac{c_2 c_3 B(k, h)^{l+1}}{c_1 \log\log p}\right\},$$

then (6.2) and (6.3) yield a contradiction. This proves (i).

For (ii), observe that if $R_{r,s,\omega_i} \ne 0$, then

$$\Omega(R_{r,s,\omega_i}) \le 2 \log |R_{r,s,\omega_i}| = O(t^2 d^h) = O(P^{1-2\epsilon} d^h),$$

and this does not depend on p. We note that $h^{-1} \ge \log d/\epsilon \log P$ implies that $\Omega(R_{r,s,\omega_i}) = o(P/\log P)$. This concludes the proof. □

REMARK 6.2. If the hypotheses of Theorem 6.1 are satisfied with $h = (\log_k N)^{1/(l+1)}$, then we recover and generalise [5, Theorem 1.2].

https://doi.org/10.1017/S000497272000009X Published online by Cambridge University Press

Acknowledgements

The author is grateful to Igor Shparlinski for helpful discussions and also to the referee for helpful suggestions.

References

[1] J. Mello, 'On quantitative estimates for quasiintegral points in orbits of semigroups of rational maps', *New York J. Math.* **25** (2019), 1091–1111.
[2] L. Mérai and I. E. Shparlinski, 'Unlikely intersections over finite fields: polynomial orbits in small subgroups', Preprint, 2019, arXiv:1904.12621.
[3] A. Ostafe and I. E. Shparlinski, 'Orbits of algebraic dynamical systems in subgroups and subfields', in: *Number Theory—Diophantine Problems, Uniform Distribution and Applications* (eds. C. Elsholtz and P. Grabner) (Springer, Cham, 2017), 347–368.
[4] A. Ostafe and M. Young, 'On algebraic integers of bounded house and preperiodicity in polynomial semigroup dynamics', Preprint, 2018, arXiv:1807.11645.
[5] I. E. Shparlinski, 'Multiplicative orders in orbits of polynomials over finite fields', *Glasg. Math. J.* **60**(2) (2018), 487–493.

JORGE MELLO, School of Mathematics and Statistics,
University of New South Wales, Kensington, NSW 2052, Australia
e-mail: j.mello@unsw.edu.au