# ORBITS LENGTHS OF MODULAR REDUCTIONS OF PAIRS OF POLYNOMIAL DYNAMICAL SYSTEMS

MEI-CHU CHANG, CARLOS D'ANDREA, ALINA OSTAFE, IGOR E. SHPARLINSKI, AND MARTÍN SOMBRA

Abstract. We obtain various bounds on orbit length of modular reductions of algebraic dynamical systems generated by polynomials with integer coefficients. In particular we extend a recent result of Chang (2015) in two different directions.

## 1. Introduction

Let

$$\boldsymbol{F} = (F_1, \ldots, F_m), \qquad F_1, \ldots, F_m \in \mathbb{K}[\boldsymbol{X}],$$

be a system of $m$ polynomials in $m$ variables $\boldsymbol{X} = (X_1, \ldots, X_m)$ over a field $\mathbb{K}$. The iterations of this system are given by

$$F_i^{(0)} = X_i \qquad \text{and} \qquad F_i^{(k)} = F_i\left(F_1^{(k-1)}, \ldots, F_m^{k-1)}\right) \tag{1.1}$$

for $i = 1, \ldots, m$ and $k \geq 1$. We refer to [AnaKhr09, Sch95, Sil07] for a background on the dynamical systems associated with these iterations.

Given a point $\boldsymbol{w} \in \mathbb{K}^m$ we define its orbit with respect to the system $\boldsymbol{F}$ as the set

$$\begin{aligned} \mathrm{Orb}_{\boldsymbol{F}}(\boldsymbol{w}) = \{\boldsymbol{w}_n \mid & \text{ with } \boldsymbol{w}_0 = \boldsymbol{w} \text{ and} \\ & \boldsymbol{w}_k = \boldsymbol{F}(\boldsymbol{w}_{k-1}),\ k = 1, 2, \ldots\}. \end{aligned} \tag{1.2}$$

The set $\mathrm{PrePer}_{\mathbb{K}}(\boldsymbol{F})$ of preperiodic points of $\boldsymbol{F}$ is the set of points $\boldsymbol{w} \in \mathbb{K}^m$ for which $\mathrm{Orb}_{\boldsymbol{F}}(\boldsymbol{w})$ is a finite set.

Sets $\mathrm{PrePer}_K(\boldsymbol{F})$ are classical objects of study and in particular for polynomial systems over $\mathbb{C}$. For example, by the celebrated result of Northcott [Nor50], if $\mathbb{K}$ is an algebraic number field, for any system of nonlinear polynomials the set $\mathrm{PrePer}_{\mathbb{K}}(\boldsymbol{F})$ is finite, see also [Sil07, Theorem 3.12]. The *Uniform Boundedness Conjecture* of Morton and Silverman [MS94] asserts that the cardinality $\#\mathrm{PrePer}_{\mathbb{K}}(\boldsymbol{F})$ can be bounded only in terms of degrees of the polynomials in $\boldsymbol{F}$ and the

---

2010 *Mathematics Subject Classification.* Primary 37P05; Secondary 11G25, 11G35, 13P15, 37P25.

*Key words and phrases.* Algebraic dynamical system, orbit length, arithmetic Nullstellensatz, resultant.

degree of $\mathbb{K}$ over $\mathbb{Q}$. Recently, several very deep results have been obtained towards this conjecture, see [BDeM11, BDeM13, GHT13, GHT15, GKN16, GKNY16, GNT15, Ing12] and references there in. In a similar spirit, Dvornicich and Zannier [DvZan07] show that under some very natural necessary conditions a polynomial $f$ may have only finitely many preperiodic points in the set $\mathcal{U}$ of roots of unity (or more generally in the cyclotomic closure $\mathbb{K}[\mathcal{U}]$ of an algebraic number field $\mathbb{K}$). On the other hand, if $\mathbb{K} = \mathbb{F}_q$ is a finite field of $q$ elements then all orbits $\mathrm{Orb}_{\boldsymbol{F}}(\boldsymbol{w})$ are finite and in fact $\#\mathrm{Orb}_{\boldsymbol{F}}(\boldsymbol{w}) \le q^m$.

We also note the result of Ingram [Ing12] which shows that the set of $t \in \overline{\mathbb{Q}}$ for which the critical points of a parametric polynomial $f_t(X) \in \mathbb{C}[X]$ are preperiodic (such polynomials are called *post-critically finite*) is a set of bounded height.

Recently, there has been active interest in the study of orbits of reductions $\boldsymbol{F}_p$ modulo distinct primes $p$ of a polynomial system $\boldsymbol{F}$ defined over $\mathbb{Q}$, see [AkbGhi09, BGH+13, Cha15, DOSS15, Sil08]. We use $\mathrm{Orb}_{\boldsymbol{F},p}(\boldsymbol{w})$ to denote the orbit of the reduction of $\boldsymbol{w} \in \mathbb{Z}^m$ modulo $p$ in the dynamical system over $\mathbb{F}_p$ generated by the reduction of polynomial system $\boldsymbol{F} \in \mathbb{Z}[\boldsymbol{X}]$ modulo $p$. Alternatively, $\mathrm{Orb}_{\boldsymbol{F},p}(\boldsymbol{w})$ is the reduction modulo $p$ of the elements of the orbit (1.2).

Silverman [Sil08] has shown that under some natural conditions on a fixed $\boldsymbol{w} \in \mathbb{Z}^m$, for almost all primes $p$ (in the sense of asymptotic relative density) we have $\#\mathrm{Orb}_{\boldsymbol{F},p}(\boldsymbol{w}) \ge (\log p)^{1+o(1)}$. This result has been improved slightly by Akbary and Ghioca [AkbGhi09].

Chang [Cha15] has given a result of a new type involving two distinct orbits. The method of [Cha15] is based on a result of Ghioca, Krieger and Nguyen [GKN16] on the finiteness of the set of $t \in \mathbb{C}$ for which $0 \in \mathrm{PrePer}_{\mathbb{C}}(f_t) \cap \mathrm{PrePer}_{\mathbb{C}}(g_t)$ for the polynomials $f_t(X) = X^d + t$ and $g_t(X) = X^d + a(t)$ with $a \in \mathbb{Z}[T]$ and a fixed integer $d \ge 2$. This result has been extended by Ghioca, Krieger, Nguyen and Ye [GKNY16] to much wider families of polynomials.

Let $\overline{\mathbb{F}}_p$ denote the algebraic closure of $\mathbb{F}_p$. Then, by [Cha15, Theorem 1], there are constants $c_1, c_2$ depending on $d$ and $a(T)$ such that for almost all primes $p$, there is a set $\mathcal{T} \subseteq \overline{\mathbb{F}}_p$ with $\#\mathcal{T} \le c_1$ such that for every $t \in \overline{\mathbb{F}}_p \setminus \mathcal{T}$ we have

$$\max\{\#\mathrm{Orb}_{f_t,p}(0), \#\mathrm{Orb}_{g_t,p}(0)\} \ge c_2 \log p. \tag{1.3}$$

Here we consider a more general case of $r \ge 1$ distinct $n$-parametric $m$-dimensional polynomial systems

$$\boldsymbol{F}_{\boldsymbol{t},\nu}(\boldsymbol{X}) = (F_{1,\nu}(\boldsymbol{X},\boldsymbol{t}), \ldots, F_{m,\nu}(\boldsymbol{X},\boldsymbol{t})), \qquad \nu = 1, \ldots, r, \tag{1.4}$$

with polynomials

$$F_{i,\nu}(\boldsymbol{X}, \boldsymbol{T}) \in \mathbb{Z}[\boldsymbol{X}; \boldsymbol{T}], \qquad i = 1, \ldots, m, \ \nu = 1, \ldots, r, \tag{1.5}$$

where $\boldsymbol{T} = (T_1, \ldots, T_n)$, specialised at the values of the parameter $\boldsymbol{t} \in \mathbb{C}^n$.

It is also convenient to denote

$$\mathbf{0}_m = (\underbrace{0, \ldots, 0}_{m}).$$

Here we extend [Cha15, Theorem 1] in several different directions:

- We use some results of [DOSS15] to obtain an analogue of the result of Chang [Cha15, Theorem 1] for $r$ distinct $n$-parametric $m$-dimensional polynomial systems $\boldsymbol{F}_{\boldsymbol{t},\nu}$, $\nu = 1, \ldots, r$, for which
$$\mathbf{0}_m \in \bigcap_{\nu=1}^{r} \mathrm{PrePer}_{\mathbb{C}}(\boldsymbol{F}_{\boldsymbol{t},\nu})$$
for only finitely many values of the parameter $\boldsymbol{t} \in \mathbb{C}^n$;
- We obtain a somewhat dual result of similar flavour, which applies to one polynomial system and several initial points.
- We use a result on divisibility of resultants which is due to Gómez-Pérez, Gutierrez, Ibeas and Sevilla [GGIS09] in the settings of [Cha15] with two parametric families of univariate polynomials to get a trade-off between the size of the exceptional set $\mathcal{T} \subseteq \overline{\mathbb{F}}_p$ and $\max\{\#\mathrm{Orb}_{f_t,p}(0), \#\mathrm{Orb}_{g_t,p}(0)\}$ in [Cha15, Theorem 1].

Note that our results can be derived for any fixed initial point $\boldsymbol{w}_0 \in \mathbb{Z}^m$, not necessary for $\boldsymbol{w}_0 = \mathbf{0}_m$. In fact no special adjstment is needed, one simply considers the polynomial systems $\boldsymbol{F}_{\boldsymbol{t},\nu}(\boldsymbol{X} - \boldsymbol{w}_0) + \boldsymbol{w}_0$, $\nu = 1, \ldots, r$, with shifted arguments and polynomials.

Throughout the paper, given functions

$$\Phi, \Psi \colon \mathbb{N} \to \mathbb{N},$$

the symbols $\Phi = O(\Psi)$ and $\Phi \ll \Psi$ both mean that there is a constant $c \geq 0$ such that $\Phi(k) \leq c\Psi(k)$ for all $k \in \mathbb{N}$. To emphasise the dependence of the implied constant $c$ on a list of parameters $\boldsymbol{\rho}$, we write $\Phi = O_{\boldsymbol{\rho}}(\Psi)$ or $\Phi \ll_{\boldsymbol{\rho}} \Psi$.

## 2. Main results

### 2.1. Multivariate systems.

We start with a generalisation of the result of Chang [Cha15, Theorem 1] and obtain a version of the lower bound (1.3) for several parametric multivariate polynomial systems as in (1.4) and (1.5).

**Theorem 2.1.** *Let $\boldsymbol{F}_{\boldsymbol{t},\nu}$, $\nu = 1,\ldots,r$, be $r \geq 1$ parametric systems of polynomials as in (1.4) and (1.5) with*

$$\max_{\substack{i=1,\ldots,m\\ \nu=1,\ldots,r}} \deg F_{i,\nu} \leq d \qquad \text{and} \qquad \max_{\substack{i=1,\ldots,m\\ \nu=1,\ldots,r}} \mathrm{h}(F_{i,\nu}) \leq h.$$

*Assume that there exists $K \in \mathbb{N}$ such that*

$$\#\left\{\boldsymbol{t} \in \mathbb{C}^n \ : \ \mathbf{0}_m \in \bigcap_{\nu=1}^{r} \mathrm{PrePer}_{\mathbb{C}}(\boldsymbol{F}_{\boldsymbol{t},\nu})\right\} \leq K.$$

*Then, for any integer $L$, there exists an integer $\mathfrak{A} \geq 1$ with*

$$\log \mathfrak{A} \ll_{d,h,n,m,r} \left(Ld^L\right)^{3n+2}$$

*such that for a prime $p$ with $p \nmid \mathfrak{A}$, for all but at most $K$ values of $\boldsymbol{t} \in \overline{\mathbb{F}}_p^n$, we have*

$$\max\left\{\#\mathrm{Orb}_{\boldsymbol{F}_{\boldsymbol{t},\nu},p}(\mathbf{0}_m) \ : \ \nu = 1,\ldots,r\right\} > L.$$

**Corollary 2.2.** *Under the conditions of Theorem 2.1, for any prime $p$ we have*

$$\max\left\{\#\mathrm{Orb}_{\boldsymbol{F}_{\boldsymbol{t},\nu},p}(\mathbf{0}_m) \ : \ \nu = 1,\ldots,r\right\} \gg_{d,h,m,n,r} \log\log p$$

*for all but at most $K$ values of $\boldsymbol{t} \in \overline{\mathbb{F}}_p^n$.*

For almost all primes, we have a stronger result.

**Corollary 2.3.** *Under the conditions of Theorem 2.1, for any fixed $\varepsilon > 0$ and sufficiently large integer $Q \geq 2$, for all but $Q^{\varepsilon}$ primes $p \leq Q$ we have*

$$\max\left\{\#\mathrm{Orb}_{\boldsymbol{F}_{\boldsymbol{t},\nu},p}(\mathbf{0}_m) \ : \ \nu = 1,\ldots,r\right\} \gg_{d,h,m,n,r} \log p$$

*for all but at most $K$ values of $\boldsymbol{t} \in \overline{\mathbb{F}}_p^n$.*

It is interesting to compare the bound of Corollary 2.3 with the result of Silverman [Sil08] and its improvement due to Akbary and Ghioca [AkbGhi09].

We now obtain a dual result for a polynomial system but with several initial points.

**Theorem 2.4.** *Let $\{\boldsymbol{F}_{\boldsymbol{t}}\}_{\boldsymbol{t}\in\mathbb{C}^n} = \{(F_1(\boldsymbol{X},\boldsymbol{t}),\ldots,F_m(\boldsymbol{X},\boldsymbol{t}))\}_{\boldsymbol{t}\in\mathbb{C}^n}$ be a parametric system with polynomials as in (1.4) and (1.5) and let $\boldsymbol{a}_\nu \in \mathbb{Z}^m$, $\nu = 1,\ldots,r$, be $r$ integer vectors with*

$$\max_{i=1,\ldots,m} \deg F_i \leq d \qquad \text{and} \qquad \max_{\substack{i=1,\ldots,m\\ \nu=1,\ldots,r}} \{\mathrm{h}(F_i), \mathrm{h}(\boldsymbol{a}_\nu)\} \leq h.$$

*Assume that there exists $K \in \mathbb{N}$ such that*

$$\#\left\{\boldsymbol{t} \in \mathbb{C}^n \ : \ \{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_r\} \subseteq \mathrm{PrePer}_{\mathbb{C}}(\boldsymbol{F}_{\boldsymbol{t}})\right\} \leq K.$$

*Then, for any integer $L$, there exists an integer $\mathfrak{A} \ge 1$ with*

$$\log \mathfrak{A} \ll_{d,h,n,m,r} \left(Ld^L\right)^{3n+2}$$

*such that for a prime $p$ with $p \nmid \mathfrak{A}$, for all but at most $K$ values of $\boldsymbol{t} \in \overline{\mathbb{F}}_p^n$, we have*

$$\max \{\#\mathrm{Orb}_{\boldsymbol{F_t},p}(\boldsymbol{a}_\nu) \ : \ \nu = 1, \dots, r\} > L.$$

For a parametric system $\{\boldsymbol{F_t}\}_{\boldsymbol{t} \in \mathbb{C}^n}$ with polynomials defined over $\mathbb{C}$ as in (1.4) and (1.5) and $\boldsymbol{a}_\nu \in \mathbb{C}^m$, $\nu = 1, \dots, r$, it is certainly desirable to control the finiteness of the set

$$\{\boldsymbol{t} \in \mathbb{C}^n \ : \ \{\boldsymbol{a}_1, \dots, \boldsymbol{a}_r\} \subseteq \mathrm{PrePer}_{\mathbb{C}}(\boldsymbol{F_t})\},$$

as well as the uniform boundedness of this set, as required in Theorem 2.4.

For instance, Baker and DeMarco [BDeM11, Theorem 1.1] prove that for any fixed $a_1, a_2 \in \mathbb{C}$ and any integer $d \ge 2$, the set of $t \in \mathbb{C}$ such that $a_1, a_2$ are preperiodic for $f_t(X) = X^d + t$ is infinite if and only if $a_1^d = a_2^d$. Thus this gives an example of polynomials to which Theorem 2.4 applies.

2.2. **Univariate systems.** In the case of the univariate systems with $\boldsymbol{X} = X$ and a univariate parameter $\boldsymbol{T} = T$ (that is, for $m = 1$, $n = 1$), we also extend the result of Chang [Cha15, Theorem 1] in a different direction.

**Theorem 2.5.** *Let $\{f_t\}_{t \in \mathbb{C}}$ and $\{g_t\}_{t \in \mathbb{C}}$ be two parametric families of univariate polynomials defined by (1.4) and (1.5) with polynomials $f(X,T), g(X,T) \in \mathbb{Z}[X,T]$ of degree at most $d$ and of height at most $h$. Assume that the following set is finite and satisfies*

$$\# \{t \in \mathbb{C} \ : \ 0 \in \mathrm{PrePer}_{\mathbb{C}}(f_t) \cap \mathrm{PrePer}_{\mathbb{C}}(g_t)\} \le K.$$

*Then, for any integer $L$, there exists an integer $\mathfrak{B} \ge 1$ with*

$$\log \mathfrak{B} \ll_{d,h} L^2 d^{2L}$$

*such that for a prime $p$ and a positive integer $N$ with $p^N \nmid \mathfrak{B}$, for all but at most $N + K - 1$ values of $t \in \overline{\mathbb{F}}_p$ we have*

$$\max \{\#\mathrm{Orb}_{f_t,p}(0), \#\mathrm{Orb}_{g_t,p}(0)\} > L.$$

As in [Cha15], we note that by the result of Ghioca, Krieger and Nguyen [GKN16] the conditions of Theorem 2.5 are satisfied for the pair of polynomials $f_t(X) = X^d + t$ and $g_t(X) = X^d + a(t)$ with $a \in \mathbb{Z}[T]$ which is not of the form $a(T) = \zeta T$, where $\zeta^{d-1} = 1$, see also [GKNY16] for a much broader family of examples.

We also have:

**Corollary 2.6.** *Under the conditions of Theorem 2.5, for any integers* $E, L, Q \geq 1$ *the number* $R$ *of primes* $p \in [Q, 2Q]$ *such that*

$$\max\{\#\mathrm{Orb}_{f_t,p}(0), \#\mathrm{Orb}_{g_t,p}(0)\} \leq L$$

*for at least* $E$ *values of* $t \in \overline{\mathbb{F}}_p$, *satisfies*

$$ER \ll_{d,h} L^2 d^{2L}/\log Q + K.$$

For example, we see that for any function $\psi$ with $\psi(z) \to \infty$ as $z \to \infty$ for all but $o(Q/\log Q)$ primes $p \in [Q, 2Q]$ we have

$$\max\{\#\mathrm{Orb}_{f_t,p}(0), \#\mathrm{Orb}_{g_t,p}(0)\} \leq \frac{\log Q - 2\log\log Q}{2\log d} - \psi(Q)$$

for at most $K + O_{d,h}(1)$ values of $t \in \overline{\mathbb{F}}_p$, which is a more explicit form of the bound (1.3).

**Theorem 2.7.** *Let* $\{f_t\}_{t\in\mathbb{C}}$ *be a parametric family of univariate polynomials defined by (1.4) and (1.5) with a polynomial* $f(X,T) \in \mathbb{Z}[X,T]$ *and let* $a, b \in \mathbb{Z}^m$ *betwo integers with*

$$\deg f \leq d \qquad \text{and} \qquad \max\{\mathrm{h}(f), \log|a|, \log|b|\} \leq h.$$

*Assume that there exists* $K \in \mathbb{N}$ *such that*

$$\#\{t \in \mathbb{C}^n \ : \ \{a, b\} \subseteq \mathrm{PrePer}_{\mathbb{C}}(f_t)\} \leq K.$$

*Then, for any integer* $L$, *there exists an integer* $\mathfrak{B} \geq 1$ *with*

$$\log \mathfrak{B} \ll_{d,h,m} L^2 d^{2L}$$

*such that for a prime* $p$ *and a positive integer* $N$ *with* $p^N \nmid \mathfrak{B}$, *for all but at most* $N + K - 1$ *values of* $t \in \overline{\mathbb{F}}_p$ *we have*

$$\max\{\#\mathrm{Orb}_{f_t,p}(a), \#\mathrm{Orb}_{f_t,p}(b)\} > L.$$

As we have mentioned, the result of Baker and DeMarco [BDeM11, Theorem 1.1] shows that the class of polynomials to which Theorem 2.7 applies is not void.

Finally, as before, we also have:

**Corollary 2.8.** *Under the conditions of Theorem 2.7, for any integers* $E, L, Q \geq 1$ *the number* $R$ *of primes* $p \in [Q, 2Q]$ *such that*

$$\max\{\#\mathrm{Orb}_{f_t,p}(a), \#\mathrm{Orb}_{f_t,p}(b)\} \leq L$$

*for at least* $E$ *values of* $t \in \overline{\mathbb{F}}_p$, *satisfies*

$$ER \ll_{d,h} L^2 d^{2L}/\log Q + K.$$

## 3. Auxiliary results

3.1. **Heights of polynomials and their iterates.** For an integer vector $\boldsymbol{a} = (a_1, \ldots, a_\ell) \in \mathbb{Z}^\ell$ we define its height $\mathrm{h}(\boldsymbol{a})$ as

$$\mathrm{h}(\boldsymbol{a}) = \max_{j=1,\ldots,\ell} \log \max\{1, |a_j|\}.$$

For a polynomial $\Psi \in \mathbb{Z}[\boldsymbol{X}]$, we define its *height*, denoted by $\mathrm{h}(\Psi)$, as the height of the vector formed by its coefficients.

The following bound on the height of a product of polynomials is important for our results. It follows from [KPS01, Lemma 1.2].

**Lemma 3.1.** *Let $\Psi_1, \ldots, \Psi_s \in \mathbb{Z}[\boldsymbol{Z}]$ be polynomials in $n$ variables $\boldsymbol{Z} = (Z_1, \ldots, Z_n)$. Then*

$$-2\sum_{i=1}^{s} \deg \Psi_i \log(n+1) \le \mathrm{h}\left(\prod_{i=1}^{s} \Psi_i\right) - \sum_{i=1}^{s} \mathrm{h}(\Psi_i) \le \sum_{i=1}^{s} \deg \Psi_i \log(n+1).$$

We also frequently use the trivial bound on the height of a sum of polynomials

$$\mathrm{h}\left(\sum_{i=1}^{s} \Psi_i\right) \le \max_{i=1,\ldots,s} \mathrm{h}(\Psi_i) + \log s. \tag{3.1}$$

Moreover, we need a bound of [DOSS15] on the degree and height of iterations of polynomial systems.

**Lemma 3.2.** *Let $\Psi_1, \ldots, \Psi_s \in \mathbb{Z}[\boldsymbol{Z}]$ be polynomials in $s$ variables $\boldsymbol{Z} = (Z_1, \ldots, Z_s)$ of degree at most $D \ge 2$ and of height at most $H$. Then, for any positive integer $k$, the polynomials $\Psi_1^{(k)}, \ldots, \Psi_s^{(k)}$ defined as in (1.1), are of degree at most*

$$\max_{j=1,\ldots,s} \deg \Psi_j^{(k)} \le D^k$$

*and of height at most*

$$\max_{j=1,\ldots,s} \mathrm{h}\left(\Psi_j^{(k)}\right) \le H\frac{D^k - 1}{D - 1} + D(D+1)\frac{D^{k-1} - 1}{D - 1}\log(s+1).$$

3.2. **Modular reduction of systems of polynomial equations.** We recall the following result of [DOSS15] concerning the reduction modulo prime numbers of systems of multivariate polynomials over the integers.

**Lemma 3.3.** *Let $\Psi_1, \ldots, \Psi_s \in \mathbb{Z}[\boldsymbol{T}]$ in $n$ variables $\boldsymbol{T} = (T_1, \ldots, T_n)$ of degree at most $D \geq 2$ and of height at most $H$, whose zero set in $\mathbb{C}^n$ has a finite number $K$ of distinct points. Then there exists $\mathfrak{A} \in \mathbb{N}$ satisfying*

$$\log \mathfrak{A} \leq C_1(n) D^{3n+1} H + C_2(n,s) D^{3n+2},$$

*with*

$$C_1(n) = 11n + 4 \qquad \text{and} \qquad C_2(n,s) = (55n + 99)\log((2n+5)s)$$

*and such that, if $p$ is a prime number not dividing $\mathfrak{A}$, then the zero set in $\overline{\mathbb{F}}_p^n$ of the system of polynomials $\Psi_i \pmod p$, $i = 1, \ldots, s$, consists of exactly $K$ distinct points.*

3.3. **Common zeros and resultants of polynomials.** One of our main results relies on a generalisation of the well known fact that if two univariate polynomials $f(T), g(T) \in \mathbb{Z}[T]$ have a common zero modulo $p$ then their resultant $\mathrm{Res}(f,g)$ is divisible by $p$. We need the following extension of this property, due to Gómez-Pérez, Gutierrez, Ibeas and Sevilla [GGIS09], to polynomials with several common roots modulo a prime.

**Lemma 3.4.** *Let $p$ be a prime and let $f, g \in \mathbb{Z}[T]$ be two univariate polynomials such that their reduction modulo $p$ do not vanish identically and have at least $N$ common roots in $\overline{\mathbb{F}}_p$ counted with multiplicities. Then $p^N \mid \mathrm{Res}(f,g)$.*

We remark that for applications, the result of [KS99, Lemma 5.3] (which counts only simple roots) is sufficient.

## 4. Proofs of main results

4.1. **Proof of Theorem 2.1.** Consider the systems

$$\boldsymbol{R}_\nu = (F_{1,\nu}(\boldsymbol{X}, \boldsymbol{T}), \ldots, F_{m,\nu}(\boldsymbol{X}, \boldsymbol{T}), T_1, \ldots, T_n), \qquad \nu = 1, \ldots, r,$$

of $m + n$ polynomials in $m + n$ variables, each.

Let $\mathcal{T}$ be set of those $\boldsymbol{t} \in \mathbb{C}^n$ for which $\mathbf{0}_m$ is a preperiodic point of every system $\boldsymbol{F}_{\boldsymbol{t},\nu}$, $\nu = 1, \ldots, r$. By our assumptions, we have that $\#\mathcal{T} \leq K$.

For every choice of nonnegative integers $k_1, \ldots, k_r < L$, we consider the system of $(m+n)r$ equations formed by the iterations

$$\boldsymbol{R}_\nu^{(L)}(\mathbf{0}_m, \boldsymbol{T}) = \boldsymbol{R}_\nu^{(k_\nu)}(\mathbf{0}_m, \boldsymbol{T}), \qquad \nu = 1, \ldots, r. \tag{4.1}$$

Observe that in each group of $m + n$ equations corresponding to the same value of $\nu$, the bottom $n$ equations in (4.1) are automatically satisfied. So we have $mr$ equations in $n$ variables:

$$F_{i,\nu}^{(L)}(\mathbf{0}_m, \boldsymbol{T}) = F_{i,\nu}^{(k_\nu)}(\mathbf{0}_m, \boldsymbol{T}) \qquad i = 1, \ldots, m, \ \nu = 1, \ldots, r. \tag{4.2}$$

Furthermore, we consider now the system of $mr$ equations

$$\prod_{k_\nu < L} \left( F_{i,\nu}^{(L)}(\mathbf{0}_m, \boldsymbol{T}) - F_{i,\nu}^{(k_\nu)}(\mathbf{0}_m, \boldsymbol{T}) \right) = 0, \qquad i = 1, \ldots, m, \ \nu = 1, \ldots, r, \tag{4.3}$$

which by the above, has at most $K$ solutions $\boldsymbol{t} \in \mathcal{T}$.

Now note that if

$$\max \left\{ \#\mathrm{Orb}_{\boldsymbol{F_t},\nu,p}(\mathbf{0}_m) \ : \ \nu = 1, \ldots, r \right\} \le L$$

for some parameter $\boldsymbol{t} \in \overline{\mathbb{F}}_p^n$, then there are some nonnegative integers $k_1, \ldots, k_r < L$ for which we have (4.1), and thus (4.3) (considered over $\overline{\mathbb{F}}_p^n$ with reductions modulo $p$ of the corresponding polynomials).

Applying Lemma 3.2 to the systems $\boldsymbol{R}_\nu$ in $n+m$ variables, we obtain that for $i = 1, \ldots, m$, $\nu = 1, \ldots, r$ and an integer $k \ge 0$ we have

$$\deg F_{i,\nu}^{(k)}(\mathbf{0}_m, \boldsymbol{T}) \le d^k \tag{4.4}$$

and

$$\mathrm{h}\left( F_{i,\nu}^{(k)}(\mathbf{0}_m, \boldsymbol{T}) \right) \le h\frac{d^k - 1}{d-1} + d(d+1)\frac{d^{k-1}-1}{d-1} \log(n+m+1). \tag{4.5}$$

From (4.4), we immediately conclude

$$\deg \left( \prod_{k<L} \left( F_{i,\nu}^{(L)}(\mathbf{0}_m, \boldsymbol{T}) - F_{i,\nu}^{(k)}(\mathbf{0}_m, \boldsymbol{T}) \right) \right) \ll_{d,h,n,m} Ld^L, \tag{4.6}$$

and furthermore by (3.1) and (4.5), we have

$$\begin{aligned}
&\mathrm{h}\left( F_{i,\nu}^{(L)}(\mathbf{0}_m, \boldsymbol{T}) - F_{i,\nu}^{(k)}(\mathbf{0}_m, \boldsymbol{T}) \right) \\
&\qquad \le h\frac{d^L - 1}{d-1} + d(d+1)\frac{d^{L-1}-1}{d-1} \log(n+m+1) + \log 2 \\
&\qquad \ll_{d,h,n,m} d^L,
\end{aligned}$$

for $i = 1, \ldots, m$ and $\nu = 1, \ldots, r$.

Hence, by Lemma 3.1, we immediately obtain

$$\mathrm{h} \left( \prod_{k<L} \left( F_{i,\nu}^{(L)}(\mathbf{0}_m, \boldsymbol{T}) - F_{i,\nu}^{(k)}(\mathbf{0}_m, \boldsymbol{T}) \right) \right) \ll_{d,h,n,m,r} Ld^L, \tag{4.7}$$

for $i = 1, \ldots, m$ and $\nu = 1, \ldots, r$.

Now we apply Lemma 3.3 with $s = mr$. Hence, if $p \nmid \mathfrak{A}$, where $\mathfrak{A}$ is as in Lemma 3.3, and thus

$$\log \mathfrak{A} \ll_{d,h,n,m,r} \left(Ld^L\right)^{3n+2}, \tag{4.8}$$

then the system (4.3) (considered over $\overline{\mathbb{F}}_p^n$ again) has at most $K$ zeros in $\overline{\mathbb{F}}_p^n$. The bound (4.8) gives the desired inequality.

4.2. **Proof of Corollary 2.2.** We can assume that $p$ is sufficiently large. Theorem 2.1 applied with

$$L = \left\lfloor \frac{\log\log p}{3(n+1)\log d} \right\rfloor$$

implies $\log \mathfrak{A} \ll_{d,h,m,n,r} (\log p)^{1-1/(3n+3)}(\log\log p)^{3n+2}$. Since $p$ is large enough we have $p \nmid \mathfrak{A}$ and the result now follows.

4.3. **Proof of Corollary 2.3.** Theorem 2.1 applied with

$$L = \left\lfloor \varepsilon \frac{\log Q}{3(n+1)\log d} \right\rfloor$$

implies $\log \mathfrak{A} \ll_{d,h,m,n,r} Q^{(1-1/(3n+3))\varepsilon}(\log Q)^{3n+2}$. The divisibility $p \mid \mathfrak{A}$ is possible for at most $2\log \mathfrak{A} \ll_{d,h,m,n,r} Q^{(1-1/(3n+3))\varepsilon}(\log Q)^{3n+2}$ primes $p$ and since $Q$ is large enough the result now follows.

4.4. **Proof of Theorem 2.4.** The proof follows the same way as for Theorem 2.1. Consider the system

$$\boldsymbol{R} = (F_1(\boldsymbol{X}, \boldsymbol{T}), \ldots, F_m(\boldsymbol{X}, \boldsymbol{T}), T_1, \ldots, T_n)$$

of $m + n$ polynomials in $m + n$ variables, each.

Let $\mathcal{T}$ be set of those $\boldsymbol{t} \in \mathbb{C}^n$ for which $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ are preperiodic points of $\boldsymbol{F_t}$. By our assumptions, we have that $\#\mathcal{T} \le K$.

For every choice of nonnegative integers $k_1, \ldots, k_r < L$, we consider the system of $(m + n)r$ equations formed by the iterations

$$\boldsymbol{R}^{(L)}(\boldsymbol{a}_\nu, \boldsymbol{T}) = \boldsymbol{R}^{(k_\nu)}(\boldsymbol{a}_\nu, \boldsymbol{T}), \qquad \nu = 1, \ldots, r. \tag{4.9}$$

Observe that in each group of equations the bottom $n$ equations in (4.1) are automatically satisfied. So we have $mr$ equation (formed by the first $m$ components of $\boldsymbol{R}^{(k_\nu)}$) in $n$ variables:

$$F_i^{(L)}(\boldsymbol{a}_\nu, \boldsymbol{T}) = F_i^{(k_\nu)}(\boldsymbol{a}_\nu, \boldsymbol{T}), \qquad i = 1, \ldots, m,\ \nu = 1, \ldots, r. \tag{4.10}$$

We consider now the system of $mr$ equations

$$\prod_{k_\nu \le L} \left(F_i^{(L)}(\boldsymbol{a}_\nu, \boldsymbol{T}) - F_i^{(k_\nu)}(\boldsymbol{a}_\nu, \boldsymbol{T})\right) = 0, \qquad i = 1, \ldots, m,\ \nu = 1, \ldots, r, \tag{4.11}$$

which by the above, has at most $K$ solutions $\boldsymbol{t} \in \mathcal{T}$.

Now note that if

$$\max\{\#\mathrm{Orb}_{\boldsymbol{F_t},p}(\boldsymbol{a}_\nu) \ : \ \nu = 1,\ldots,r\} \le L$$

for some parameter $\boldsymbol{t} \in \overline{\mathbb{F}}_p^n$, then there are some nonnegative integers $k_1,\ldots,k_r < L$ for which we have (4.9), and thus (4.11) (considered over $\overline{\mathbb{F}}_p^n$ with reductions modulo $p$ of the corresponding polynomials).

As before, applying Lemma 3.2 to the system $\boldsymbol{R}$ in $n+m$ variables, we see that for any integer $k \ge 1$ we have a full analogues of (4.6) and (4.7), that is,

$$\deg\left(\prod_{k<L}\left(F_i^{(L)}(\boldsymbol{a}_\nu,\boldsymbol{T}) - F_i^{(k)}(\boldsymbol{a}_\nu,\boldsymbol{T})\right)\right) \ll_{d,h,n,m,r} Ld^L$$

and

$$\mathrm{h}\left(\prod_{k<L}\left(F_i^{(L)}(\boldsymbol{a}_\nu,\boldsymbol{T}) - F_i^{(k)}(\boldsymbol{a}_\nu,\boldsymbol{T})\right)\right) \ll_{d,h,n,m,r} Ld^L,$$

for $i = 1,\ldots,m$ and $\nu = 1,\ldots,r$.

Now we apply Lemma 3.3 with $s = mr$. Hence, if $p \nmid \mathfrak{A}$, where $\mathfrak{A}$ is as in Lemma 3.3, and thus

$$\log \mathfrak{A} \ll_{d,h,n,m,r} \left(Ld^L\right)^{3n+2}, \qquad (4.12)$$

then the system (4.11) (considered over $\overline{\mathbb{F}}_p^n$ again) has at most $K$ zeros in $\overline{\mathbb{F}}_p^n$. The bound (4.12) gives the desired inequality.

4.5. **Proof of Theorem 2.5.** As in Theorem 2.1, consider the two dimensional dynamical systems

$$\boldsymbol{R} = (f(X,T),T), \qquad \text{and} \qquad \boldsymbol{Q} = (g(X,T),T).$$

By the finiteness assumption, the polynomials

$$\Phi_L(T) = \prod_{k=0}^{L-1}\left(f^{(L)}(0,T) - f^{(k)}(0,T)\right),$$
$$\Psi_L(T) = \prod_{k=0}^{L-1}\left(g^{(L)}(0,T) - g^{(k)}(0,T)\right),$$

have at most $K$ common zeros $t \in \mathbb{C}$. This implies that at least one among $\Phi_L(T)$ and $\Psi_L(T)$ is not zero. If one of them is identically zero, then the degree of the other is bounded by $K$ and the claim follows straightforwardly by taking $\mathfrak{B} = 1$.

Suppose then without loss of generality that $\Psi_L(T) \neq 0 \neq \Phi_L(T)$, and write

$$\Phi_L(T) = \widetilde{\Phi}_L(T) H_L(T) \qquad \text{and} \qquad \Psi_L(T) = \widetilde{\Psi}_L(T) H_L(T),$$

for nonzero polynomials $\widetilde{\Phi}_L(T), \widetilde{\Psi}_L(T), H_L(T) \in \mathbb{Z}[T]$ such that the polynomials $\widetilde{\Phi}_L(T)$ and $\widetilde{\Psi}_L(T)$ have no common root in $\mathbb{C}$ and $H_L(T)$ has at most $K$ distinct zeros.

Let $M$ the number of their common zeros in $\overline{\mathbb{F}}_p$. At most $K$ of them come from the polynomial $H_L(T)$. Hence, the polynomials, $\widetilde{\Phi}_L(T)$ and $\widetilde{\Psi}_L(T)$ have at least $M-K$ common zeros.

In particular, by Lemma 3.4, we deduce that $p^{M-K} \mid \mathfrak{B}$, where

$$\mathfrak{B} = \left| \mathrm{Res}\left(\widetilde{\Phi}_L(T), \widetilde{\Psi}_L(T)\right) \right| > 0.$$

Hence, for a bound $N$ such that $p^N \nmid \mathfrak{B}$, we must have $M \leq N+K-1$. One checks that this is also true if one of the polynomials $\widetilde{\Phi}_L(T)$ and $\widetilde{\Psi}_L(T)$ vanishes identically modulo $p$.

To finish the proof we need to bound the size of $\mathfrak{B}$. As in the proof of Theorem 2.1, applying Lemma 3.2 to the system $\boldsymbol{R}$ and $\boldsymbol{Q}$ in two variables, we get

$$\deg \Phi_L, \ \deg \Psi_L \leq L d^L$$

and

$$\mathrm{h}\left(\Phi_L(T)\right), \ \mathrm{h}\left(\Psi_L(T)\right) \ll_{d,h} L d^L. \tag{4.13}$$

We apply now Lemma 3.1 and using (4.13), we conclude that

$$\mathrm{h}(\widetilde{\Phi}_L), \mathrm{h}(\widetilde{\Psi}_L) \ll_{d,h} L d^L. \tag{4.14}$$

We now use the trivial bound

$$|\det B| \leq s! H^s \leq s^s H^s$$

on the determinant of an $s \times s$ matrix $B$ with complex entries of absolute value at most $H$ (note that the Hadamard inequality does not lead to any advantage here). We apply it to the Sylvester determinant formula for the resultant $\mathfrak{B}$ (with $\log H \ll_{d,h,m} L d^L$ and $s \leq L d^L$). Hence we derive

$$\log \mathfrak{B} \ll_{d,h} L^2 d^{2L},$$

which concludes the proof.

4.6. **Proof of Corollary 2.6.** Theorem 2.5 implies

$$(E-K+1) R \log Q \leq \log \mathfrak{A} \ll_{d,h} L^2 d^{2L}$$

and the result now follows.

4.7. **Proof of Theorem 2.7.** By consider the polynomials

$$\Phi_L(T) = \prod_{k=0}^{L-1} \left(f^{(L)}(a,T) - f^{(k)}(a,T)\right),$$
$$\Psi_L(T) = \prod_{k=0}^{L-1} \left(f^{(L)}(b,T) - g^{(k)}(b,T)\right),$$

which have at most $K$ common zeros $t \in \mathbb{C}$, and then follow the same argument as in the proof of Theorem 2.5. In particular, we have full analogues of the bounds (4.13) and (4.14).

4.8. **Proof of Corollary 2.8.** Similarly to the proof of Corollary 2.6 we note that Theorem 2.7 implies

$$(E - K + 1)R \log Q \le \log \mathfrak{A} \ll_{d,h} L^2 d^{2L}$$

and the result now follows.

## 5. Comments

We remark that considering the systems of equations (4.2) and (4.10) separately for each choice of the parameters $k_1, \ldots, k_r$ and $k$, respectively, instead of the systems of equations (4.3) and (4.11), one can slightly improve polynomial factors in the dependence on $L$ in the bounds of Theorems 2.1 and 2.4.

## References

[AkbGhi09] A. Akbary and D. Ghioca, 'Periods of orbits modulo primes', *J. Number Theory*, **129** (2009), 2831–2842.

[AnaKhr09] V. Anashin and A. Khrennikov, *Applied algebraic dynamics* , Walter de Gruyter, 2009.

[BDeM11] M. Baker and L. DeMarco, 'Preperiodic points and unlikely intersections', *Duke Math. J.*, **159** (2011), 1–29.

[BDeM13] M. Baker and L. DeMarco, 'Special curves and post-critically finite polynomials', *Forum Math., Pi*, **1** (2013), e3, 1–35.

[BGH+13] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon and T. J. Tucker, 'Periods of rational maps modulo primes', *Math. Ann.*, **355** (2013), 637–660.

[Cha15] M.-C. Chang, 'On periods modulo p in arithmetic dynamics', *C. R. Acad. Sci. Paris, Ser. I*, **353** (2015), 283–285.

[DKS13] C. D'Andrea, T. Krick and M. Sombra, 'Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze', *Ann. Sci. Éc. Norm. Supér.*, **46** (2013), 549–627.

[DOSS15] C. D'Andrea, A. Ostafe, I. Shparlinski and M. Sombra, 'Reduction modulo primes of systems of polynomial equations and algebraic dynamical systems', *Preprint*, 2015 (see http://arxiv.org/1505.05814)

[DvZan07] R. Dvornicich and U. Zannier, 'Cyclotomic Diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps)', *Duke Math. J.* **139** (2007), 527–554.

[GGIS09] D. Gómez-Pérez, J. Gutierrez, A. Ibeas and D. Sevilla, 'Common factors of resultants modulo $p$', *Bull. Aust. Math. Soc.*, **79** (2009), 299–302.

[GHT13] D. Ghioca, L.-C. Hsia and T. J. Tucker, 'Preperiodic points for families of polynomials', *Algebra Number Theory*, **7** (2013), 701–732.

[GHT15] D. Ghioca, L.-C. Hsia and T. J. Tucker, 'Preperiodic points for families of rational maps', *Proc. London Math. Soc.*, **110** (2015), 395–427.

[GKN16] D. Ghioca, H. Krieger and K. Nguyen, 'A case of the dynamical André-Oort conjecture', *Internat. Math. Res. Notices*, **2016** (2016), 738–758.

[GKNY16] D. Ghioca, H. Krieger, K. Nguyen and H. Ye, 'The dynamical André-Oort conjecture: Unicritical polynomials', *Duke Math. J.* (to appear).

[GNT15] D. Ghioca, K. Nguyen nd T. Tucker, 'Portraits of preperiodic points for rational maps', *Math. Proc. Cambridge Philos. Soc.*, **159** (2015), 165–186.

[Ing12] P. Ingram, 'A finiteness result for post-critically finite polynomials', *Int. Math. Res. Not.* (2012), 524–543.

[KS99] S. V. Konyagin and I. E. Shparlinski, 'Character sums with exponential functions and their applications', *Cambridge Univ. Press,* Cambridge, 1999.

[KPS01] T. Krick, L. M. Pardo, and M. Sombra, 'Sharp estimates for the arithmetic Nullstellensatz', *Duke Math. J.* **109** (2001), 521–598.

[MS94] P. Morton and J. H. Silverman, 'Rational periodic points of rational function', *Internat. Math. Res. Notices*, **1994** (1994), 97–110.

[Nor50] D. G. Northcott, 'Periodic points on an algebraic variety', *Ann. of Math.*, **51** (1950) 167–177.

[Sch95] K. Schmidt, *Dynamical systems of algebraic origin*, Progress in Math., vol. 128, Birkhäuser Verlag, 1995.

[Sil07] J. H. Silverman, *The arithmetic of dynamical systems*, Springer Verlag, 2007.

[Sil08] J. H. Silverman, 'Variation of periods modulo $p$ in arithmetic dynamics', *New York J. Math.*, **14** (2008), 601–616.

[Zan09] U. Zannier, *Lecture notes on Diophantine analysis, With an appendix by Francesco Amoroso*, Lecture Notes. Scuola Normale Superiore di Pisa (New Series), 8, Edizioni della Normale, Pisa, 2009.

Department of Mathematics, University of California. Riverside, CA 92521, USA
*E-mail address*: mcc@math.ucr.edu
*URL*: http://mathdept.ucr.edu/faculty/chang.html

Departament de Matemàtiques i Informàtica, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain
*E-mail address*: cdandrea@ub.edu
*URL*: http://atlas.mat.ub.es/personals/dandrea

School of Mathematics and Statistics, University of New South Wales. Sydney, NSW 2052, Australia
*E-mail address*: alina.ostafe@unsw.edu.au
*URL*: http://web.maths.unsw.edu.au/~alinaostafe

School of Mathematics and Statistics, University of New South Wales. Sydney, NSW 2052, Australia
*E-mail address*: igor.shparlinski@unsw.edu.au
*URL*: http://web.maths.unsw.edu.au/~igorshparlinski

ICREA and Departament de Matemàtiques i Informàtica, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain
*E-mail address*: sombra@ub.edu
*URL*: http://atlas.mat.ub.es/personals/sombra