

ORBITS OF POLYNOMIAL DYNAMICAL SYSTEMS MODULO PRIMES

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

ABSTRACT. We present lower bounds for the orbit length of reduction modulo primes of parametric polynomial dynamical systems defined over the integers, under a suitable hypothesis on its set of preperiodic points over \mathbb{C} . Applying recent results of Baker and DeMarco (2011) and of Ghioca, Krieger, Nguyen and Ye (2017), we obtain explicit families of parametric polynomials and initial points such that the reductions modulo primes have long orbits, for all but a finite number of values of the parameters. This generalizes a previous lower bound due to Chang (2015). As a by-product, we also slightly improve a result of Silverman (2008) and recover a result of Akbary and Ghioca (2009) as special extreme cases of our estimates.

1. INTRODUCTION

Recently, there has been active interest in the study of orbits of reductions modulo primes of algebraic dynamical systems defined over \mathbb{Q} , see [AkbGhi09, BGH+13, Cha15, DOSS15, Sil08]. In this paper, we obtain lower bounds for the orbit length of the reduction modulo primes of dynamical systems defined by polynomials with integer coefficients, under a suitable hypothesis on its set of preperiodic points over \mathbb{C} .

One of the first results in this subject is due to Silverman [Sil08], where he studies the orbit length for the the reduction modulo a prime p of a dynamical system on a quasiprojective variety over a number field and a non-preperiodic point. In particular, he gives a weak lower bound for the length of these orbits that is satisfied for every p [Sil08, Corollary 12], and a stronger one that is satisfied for almost all p , in the sense of the analytic density [Sil08, Theorem 1]. This latter lower bound has been slightly improved by Akbary and Ghioca [AkbGhi09], who also show that it holds for almost all p in the sense of the natural density of primes.

In [Cha15], Chang has given a result of a new type involving two distinct orbits. Let $F = X^d + T$, $G = X^d + a \in \mathbb{Z}[X, T]$ for a fixed integer $d \geq 2$ and $a \in \mathbb{Z}[T] \setminus \mathbb{Z}$ with $a^{d-1} \neq T^{d-1}$. For a prime p , we denote by $\overline{\mathbb{F}}_p$ the algebraic closure of \mathbb{F}_p . For $t \in \overline{\mathbb{F}}_p$, we set F_t for the map $\overline{\mathbb{F}}_p \rightarrow \overline{\mathbb{F}}_p$ defined by $x \mapsto F_t(x) = F(x, t)$, and similarly for G_t . By [Cha15, Theorem 1], there are constants $c_1, c_2 > 0$ depending only on d and a such that, for almost all p (in the sense of the natural density of primes) there is a set $\mathcal{T} \subseteq \overline{\mathbb{F}}_p$ with $\#\mathcal{T} \leq c_1$ such that, for all $t \in \overline{\mathbb{F}}_p \setminus \mathcal{T}$,

$$(1.1) \quad \max \{ \#\text{Orb}_{F_t}(0), \#\text{Orb}_{G_t}(0) \} \geq c_2 \log p,$$

where $\text{Orb}_{F_t}(0)$ and $\text{Orb}_{G_t}(0)$ denote the orbits of the point $0 \in \overline{\mathbb{F}}_p$ in the dynamical systems given by the iterations of F_t and of G_t , respectively. This theorem relies on

Date: February 8, 2017.

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

Key words and phrases. Algebraic dynamical system, preperiodic point, orbit length, polynomial equations, resultant.

a previous result of Ghioca, Krieger and Nguyen [GKN16] on the finiteness of the set of $t \in \mathbb{C}$ for which $0 \in \text{PrePer}_{\mathbb{C}}(F_t) \cap \text{PrePer}_{\mathbb{C}}(G_t)$, the intersection of the sets of preperiodic points of F_t and of G_t .

Inspired by this result, in the present paper we study the length of the orbits of the reduction of several parametric dynamical systems and several starting points. In more precise terms, let $\mathbf{X} = (X_1, \dots, X_m)$ and $\mathbf{T} = (T_1, \dots, T_n)$ be groups of variables and, for $\nu = 1, \dots, r$, let $\mathbf{F}_{\nu} = (F_{\nu,1}, \dots, F_{\nu,m}) \in \mathbb{Z}[\mathbf{X}, \mathbf{T}]^m$, that we consider as family of n -parametric systems of m -variate polynomials. Indeed, given a field \mathbb{K} and a point $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{K}^n$, we denote by $\mathbf{F}_{\mathbf{t}}$ the map $\mathbb{K}^m \rightarrow \mathbb{K}^m$ defined, for $\mathbf{x} \in \mathbb{K}^m$, by $\mathbf{F}_{\mathbf{t}}(\mathbf{x}) = \mathbf{F}(\mathbf{x}, \mathbf{t})$. Hence, the system \mathbf{F} defines an n -parametric family of polynomial dynamical systems on \mathbb{K}^m .

Given a subset $S \subseteq \mathbb{C}^m$, an important problem in this context is to understand the size and the structure of the set of points $\mathbf{t} \in \mathbb{C}^n$ such that

$$(1.2) \quad S \subseteq \bigcap_{\nu=1}^r \text{PrePer}_{\mathbb{C}}(\mathbf{F}_{\nu, \mathbf{t}}).$$

Some particular cases of this problem have been studied by Ghioca, Krieger and Nguyen [GKN16], Ghioca, Krieger, Nguyen and Ye [GKNY17], and Baker and DeMarco [BDeM11]. Indeed, the set of preperiodic points of an algebraic dynamical system over \mathbb{C} is a classical object of study. Most of the results and conjectures in this subject hint that, under suitable hypothesis, this set of preperiodic points should be rather small, see also [BDeM13, GHT13, GHT15, GNT15, Ing12]. The sparsity of these sets suggests that the set of parameters \mathbf{t} such that (1.2) holds should be small, typically finite or empty.

Our first main result in this paper (Theorem 2.1) gives a lower bound for the orbit length of the reduction modulo primes of algebraic dynamical systems depending on n parameters, under the assumption that the set of parameters $\mathbf{t} \in \mathbb{C}^n$ satisfying (1.2) for a given subset of starting integer points $S \subseteq \mathbb{Z}^m$ is finite. Our proof consists of translating the condition about the lengths of the orbits into a system of polynomial equations with integer coefficients, to which we apply a result by D'Andrea, Ostafe, Shparlinski and Sombra [DOSS15, Theorem 2.1].

As a consequence, we recover a result in [AkbGhi09], and slightly improve a result in [Sil08] (Corollaries 2.3 and 2.4). Combined with results in [GKNY17] and in [BDeM11], this gives explicit families of parametric polynomials and initial points such that the reductions modulo primes have long orbits, for all but a finite number of values for the parameters (Corollaries 2.5 and 2.6). In addition, Corollary 2.5 contains Chang's lower bound (1.1) as a particular case, and sharpens the constant c_2 therein.

Our second main result (Theorem 2.7) applies to the case $n = 1$, that is, to systems of polynomials depending on one parameter. Here, we can strengthen Theorem 2.1 to a result that is valid for every prime. Its proof follows by applying a divisibility property for the resultant of two polynomials whose reduction modulo a prime has several common roots, due to Gómez-Pérez, Gutiérrez, Ibeas and Sevilla [GGIS09].

2. STATEMENT OF THE MAIN RESULTS

Boldface symbols denote finite sets or sequences of objects, where the type and number is clear from the context. For $m \geq 1$ and $n \geq 0$ we set $\mathbf{X} = (X_1, \dots, X_m)$ and $\mathbf{T} = (T_1, \dots, T_n)$, which we consider as groups of *variables* and of *parameters*, respectively.

Given a system $\mathbf{F} = (F_1, \dots, F_m) \in \mathbb{Z}[\mathbf{X}, \mathbf{T}]^m$, its iterations are given by

$$\mathbf{F}^{(0)} = \mathbf{X} \quad \text{and} \quad \mathbf{F}^{(k)} = \mathbf{F}(\mathbf{F}^{(k-1)}, \mathbf{T}) \quad \text{for } k \geq 1.$$

For a field \mathbb{K} and a point $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{K}^n$, we consider the map

$$(2.1) \quad \mathbf{F}_{\mathbf{t}}: \mathbb{K}^m \longrightarrow \mathbb{K}^m, \quad \mathbf{x} \longmapsto \mathbf{F}(\mathbf{x}, \mathbf{t}).$$

Hence, \mathbf{F} defines an n -parametric family of polynomial dynamical systems on \mathbb{K}^m . Given a vector $\mathbf{w} \in \mathbb{K}^m$, we denote by $\text{Orb}_{\mathbf{F}_{\mathbf{t}}}(\mathbf{w})$ the *orbit* of \mathbf{w} under the map in (2.1). Such a point is *preperiodic* with respect to $\mathbf{F}_{\mathbf{t}}$ if its orbit is finite, and the set of these preperiodic points is denoted by $\text{PrePer}_{\mathbb{K}}(\mathbf{F}_{\mathbf{t}})$. We refer to [AnaKhr09, Sch95, Sil07] for a background on these dynamical systems.

As usual, we use $\text{ord}_p z$ to denote the p -adic order of $z \in \mathbb{Z}$

Although we are mostly interested in the case of n parameters with $n \geq 1$, we sometimes consider the non-parametric case when $n = 0$ (thus $\mathbb{K}^0 = \{0\}$) and recover a result in [AkbGhi09] and slightly improve another result in [Sil08].

For a vector $\mathbf{a} \in \mathbb{Z}^\ell$, we define its *height*, denoted by $h(\mathbf{a})$, as the logarithm of the maximum of the absolute values of its coordinates, if $\mathbf{a} \neq \mathbf{0}$, and as 0 otherwise. For a polynomial G with integer coefficients, its *height*, denoted by $h(G)$, is defined as the height of its vector of coefficients. For a family of polynomials $\mathbf{G} = (G_1, \dots, G_\ell)$ with integer coefficients, we respectively define its *degree* and *height* as

$$\deg \mathbf{G} = \max_{1 \leq i \leq \ell} \deg G_i \quad \text{and} \quad h(\mathbf{G}) = \max_{1 \leq i \leq \ell} h(G_i).$$

Given functions

$$f, g: \mathbb{N} \longrightarrow \mathbb{R},$$

the symbol $f \ll g$ means that there is a constant $c \geq 0$ such that $|f(k)| \leq cg(k)$ for all $k \in \mathbb{N}$. To emphasize the dependence of the implied constant c on a list of parameters ρ , we write $f \ll_\rho g$.

We first present a lower bound for the length of the orbits of reduction modulo primes of several parametric multivariate polynomial systems and several initial points.

Theorem 2.1. *Let $\mathbf{F}_\nu \in \mathbb{Z}[\mathbf{X}, \mathbf{T}]^m$, $\nu = 1, \dots, r$, be a family of $r \geq 1$ parametric systems of polynomials and $\mathbf{a}_j \in \mathbb{Z}^m$, $j = 1, \dots, s$, a family of $s \geq 1$ integer vectors, such that the set*

$$(2.2) \quad \{\mathbf{t} \in \mathbb{C}^n : \mathbf{a}_j \in \text{PrePer}_{\mathbb{C}}(\mathbf{F}_{\nu, \mathbf{t}}) \text{ for all } \nu, j\}$$

is empty if $n = 0$, or finite if $n \geq 1$. Set κ for the cardinality of this set, and let $d \geq \max\{2, \deg \mathbf{F}_\nu\}$ for all ν and $h \geq \max\{h(\mathbf{F}_\nu), h(\mathbf{a}_j)\}$ for all ν and j . Let also $L \geq 1$. Then there is an integer $\mathfrak{A}_L \geq 1$ with

$$\log \mathfrak{A}_L \ll_{m, n, r, s, h} \begin{cases} Ld^L & \text{if } n = 0, \\ L^{3n+3}d^{(3n+2)L} & \text{if } n \geq 1, \end{cases}$$

such that, for every prime p not dividing \mathfrak{A}_L , for all but at most κ values of $\mathbf{t} \in \overline{\mathbb{F}}_p^n$,

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu, \mathbf{t}}}(\mathbf{a}_j \bmod p) > L.$$

Remark 2.2. When $n = 0$, the case $r = s = 1$ already contains the cases when r and s are arbitrary. Indeed, we recall that $\mathbb{C}^0 = \{0\}$ and so $\mathbf{t} = 0$. Now, let $\mathbf{F}_\nu \in \mathbb{Z}[\mathbf{X}]^m$, $\nu = 1, \dots, r$, and $\mathbf{a}_j \in \mathbb{Z}^m$, $j = 1, \dots, s$, such that the set in (2.2) is empty. Note that accordingly to our general convention there is only one possible specialisation of \mathbf{F}_ν with $\mathbf{t} = 0$ and $\mathbf{F}_{\nu,0} = \mathbf{F}_\nu$. The previous condition then implies that there exist ν_0 and j_0 such that

$$\mathbf{a}_{j_0} \notin \text{PrePer}_{\mathbb{C}}(\mathbf{F}_{\nu_0,0}).$$

Theorem 2.1 applied to this system and this initial point implies that, for all $p \nmid \mathfrak{A}_L$,

$$\#\text{Orb}_{\mathbf{F}_{\nu,0}}(\mathbf{a}_j \bmod p) > L,$$

which gives the conclusion for the whole families \mathbf{F}_ν , $\nu = 1, \dots, r$, and \mathbf{a}_j , $j = 1, \dots, s$.

We have the following result for all primes.

Corollary 2.3. With conditions as in Theorem 2.1, for any $0 < \varepsilon < \frac{1}{(3n+2)\log d}$, there exists a constant c depending only on m, n, r, s, h and ε such that, for all $p \geq c$ and all but at most κ values of $\mathbf{t} \in \overline{\mathbb{F}}_p^n$,

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu,\mathbf{t}}}(\mathbf{a}_j \bmod p) > \varepsilon \log \log p.$$

When $n = 0$, this conclusion also holds for any $0 < \varepsilon < \frac{1}{\log d}$.

This result applied to a polynomial system $\mathbf{F} \in \mathbb{Z}[\mathbf{X}]^m$ and a point $\mathbf{a} \in \mathbb{Z}^m$ with infinite orbit with respect to the map $\mathbf{F}: \mathbb{C}^m \rightarrow \mathbb{C}^m$, shows that there is a constant $c(m, h)$ such that, for every $p \geq c(m, h)$,

$$\#\text{Orb}_{\mathbf{F}}(\mathbf{a}_j \bmod p) > \frac{\log \log p}{\log d}.$$

This refines the lower bound in [Sil08, Corollary 12] for a dynamical system on the affine space defined by polynomials with integer coefficients, by giving its explicit dependence on the degree of \mathbf{F} .

For a subset \mathcal{P} of the set of primes, its *natural density* is defined as the real number

$$\lim_{Q \rightarrow \infty} \frac{\#\{p \in \mathcal{P} : p \leq Q\}}{\#\{p \text{ prime} : p \leq Q\}},$$

whenever this limit exists. We can also deduce from Theorem 2.1 the following stronger lower bound for the length of the orbits of the system \mathbf{F} modulo a prime p that is valid for almost all primes p , in the sense of the natural density of this set.

Corollary 2.4. Under the conditions of Theorem 2.1, for any $0 < \varepsilon < \frac{1}{(3n+2)\log d}$, the set of primes p such that, for all but at most κ values of $\mathbf{t} \in \overline{\mathbb{F}}_p^n$,

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu,\mathbf{t}}}(\mathbf{a}_j \bmod p) \geq \varepsilon \log p,$$

has natural density 1. When $n = 0$, this conclusion also holds for any $0 < \varepsilon < \frac{1}{\log d}$.

For a polynomial system $\mathbf{F} \in \mathbb{Z}[\mathbf{X}]^m$ and a point $\mathbf{a} \in \mathbb{Z}^m$ with infinite orbit over \mathbb{C} , Corollary 2.4 recovers [AkbGhi09, Theorem 1.1(1)].

The result of Ghioca, Krieger, Nguyen and Ye in [GKNY17] mentioned in the introduction implies that, for $d \geq 2$ and $u, v \in \mathbb{Z}[T] \setminus \mathbb{Z}$ such that $u^{d-1} \neq v^{d-1}$, the

set of $t \in \mathbb{C}$ such that the point $0 \in \mathbb{C}$ is preperiodic both for the map $x \mapsto x^d + u(t)$ and the map $x \mapsto x^d + v(t)$, is finite.

The following result is a direct consequence of Corollaries 2.3 and 2.4. It generalizes Chang's lower bound (1.1) to a larger family of pairs of polynomials and, moreover, it refines the value of the constant c_2 in that lower bound.

Corollary 2.5. *Let $d \geq 2$ and $u, v \in \mathbb{Z}[T] \setminus \mathbb{Z}$ such that $u^{d-1} \neq v^{d-1}$. Then, for any $0 < \varepsilon < \frac{1}{5 \log d}$, there exists $\kappa \geq 0$ such that, for every sufficiently large p and all but at most κ values of $t \in \overline{\mathbb{F}}_p$,*

$$\max \left\{ \#\text{Orb}_{x^d+u(t)}(0), \#\text{Orb}_{x^d+v(t)}(0) \right\} > \varepsilon \log \log p.$$

Furthermore, the set of primes p such that, for all but at most κ values of $t \in \overline{\mathbb{F}}_p$,

$$\max \left\{ \#\text{Orb}_{x^d+u(t)}(0), \#\text{Orb}_{x^d+v(t)}(0) \right\} \geq \varepsilon \log p,$$

has natural density 1.

Another instance where our results can be applied is given by the result of Baker and DeMarco [BDeM11, Theorem 1.1] mentioned in the introduction: given $d \geq 2$ and $a_1, a_2 \in \mathbb{Z}$, the set of $t \in \mathbb{C}$ such that both a_1 and a_2 are preperiodic for the map $X \mapsto X^d + t$ is infinite if and only if $a_1^d = a_2^d$. The following result is also a direct consequence of Corollaries 2.3 and 2.4.

Corollary 2.6. *Let $d \geq 2$ and $a_1, a_2 \in \mathbb{Z}$ with $a_1^d \neq a_2^d$. Then, for any $0 < \varepsilon < \frac{1}{5 \log d}$, there exists $\kappa \geq 0$ such that, for every sufficiently large p and all but at most κ values of $t \in \overline{\mathbb{F}}_p$,*

$$\max \left\{ \#\text{Orb}_{X^d+t}(a_1 \bmod p), \#\text{Orb}_{X^d+t}(a_2 \bmod p) \right\} > \varepsilon \log \log p.$$

Furthermore, the set of primes p such that, for all but at most κ values of $t \in \overline{\mathbb{F}}_p$,

$$\max \left\{ \#\text{Orb}_{x^d+t}(a_1 \bmod p), \#\text{Orb}_{x^d+t}(a_2 \bmod p) \right\} \geq \varepsilon \log p,$$

has natural density 1.

For systems depending on a single parameter T , we can strengthen Theorem 2.1 to a result that is valid for every prime.

Theorem 2.7. *Let $\mathbf{F}_\nu \in \mathbb{Z}[\mathbf{X}, T]^m$, $\nu = 1, \dots, r$, be a family of $r \geq 1$ parametric systems of polynomials and $\mathbf{a}_j \in \mathbb{Z}^m$, $j = 1, \dots, s$, a family of $s \geq 1$ integer vectors, such that the set*

$$(2.3) \quad \{t \in \mathbb{C} : \mathbf{a}_j \in \text{PrePer}_{\mathbb{C}}(\mathbf{F}_{\nu,t}) \text{ for all } \nu, j\}$$

is finite. Set κ for the cardinality of this set, and let $d \geq \max\{2, \deg \mathbf{F}_\nu\}$ for all ν and $h \geq \max\{h(\mathbf{F}_\nu), h(\mathbf{a}_j)\}$ for all ν and j . Let also $L \geq 1$. Then there is an integer $\mathfrak{A}_L \geq 1$ with

$$\log \mathfrak{A}_L \ll_{m,r,s,h} L^2 d^{2L},$$

such that, for every prime p , for all but at most $\kappa + \text{ord}_p \mathfrak{A}_L$ values of $t \in \overline{\mathbb{F}}_p$,

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu,t}}(\mathbf{a}_j \bmod p) > L.$$

Theorem 2.7 contains Theorem 2.1 for systems depending on a single parameter, with a better control for the integer \mathfrak{A}_L : this latter result corresponds to the primes p such that $\text{ord}_p \mathfrak{A}_L = 0$.

As a consequence of Theorem 2.7, we obtain the following result valid for all primes, and which is a sharper version of Corollary 2.4 for the case of $n = 1$ parameter.

Corollary 2.8. *With conditions as in Theorem 2.7, for any $0 < \varepsilon < \frac{1}{2 \log d}$, there exists $0 < \gamma < 1$ such that, for every $Q \geq 2$ and every prime $p \leq Q$, the number of values of $t \in \overline{\mathbb{F}}_p$ such that*

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu,t}}(\mathbf{a}_j \bmod p) \leq \varepsilon \log p$$

is bounded by $\kappa + c_p$, with

$$\sum_{p \leq Q} c_p \ll_{m,n,r,s,h} Q^\gamma.$$

3. PRELIMINARIES

In this section, we gather some bounds on the heights and degrees of some polynomials. We also need some rather general statements about the reduction modulo primes of systems of multivariate polynomials and about the divisibility of resultants.

We start with bounds for the height of sums and products of polynomials, whose proof can be derived from [KPS01, Lemma 1.2].

Lemma 3.1. *Let $G_i \in \mathbb{Z}[T_1, \dots, T_n]$, $i = 1, \dots, s$. Then*

$$(1) \quad h\left(\sum_{i=1}^s G_i\right) \leq \max_{1 \leq i \leq s} h(G_i) + \log s;$$

$$(2) \quad -2 \log(n+1) \sum_{i=1}^s \deg G_i \leq h\left(\prod_{i=1}^s G_i\right) - \sum_{i=1}^s h(G_i) \leq \log(n+1) \sum_{i=1}^s \deg G_i.$$

We also need the upper bound from [DOSS15, Lemma 3.4] for the degree and the height of iterations of polynomial dynamical systems.

Lemma 3.2. *Let $G_i \in \mathbb{Z}[T_1, \dots, T_n]$, $i = 1, \dots, n$, be polynomials of degree at most $d \geq 2$ and height at most h . Set $\mathbf{G} = (G_1, \dots, G_n)$ and, for $k \geq 0$, let $\mathbf{G}^{(k)}$ denote the k -th iterate of \mathbf{G} . Then*

$$\deg \mathbf{G}^{(k)} \leq d^k \quad \text{and} \quad h\left(\mathbf{G}^{(k)}\right) \leq h \frac{d^k - 1}{d - 1} + d(d+1) \frac{d^{k-1} - 1}{d - 1} \log(n+1).$$

Crucial to our strategy is the following result on the reduction modulo primes of systems of multivariate polynomials over the integers, whose proof relies on the arithmetic Nullstellensatz from [DKS13].

Theorem 3.3 ([DOSS15, Theorem 2.1]). *Let $G_i \in \mathbb{Z}[T_1, \dots, T_n]$, $i = 1, \dots, s$, be $n \geq 1$ polynomials of degree at most $d \geq 2$ and height at most h , whose zero set in \mathbb{C}^n has a finite number κ of distinct points. Then there is an integer $\mathfrak{A} \geq 1$ with*

$$\log \mathfrak{A} \leq (11n + 4)d^{3n+1}h + (55n + 99) \log((2n + 5)s)d^{3n+2}$$

such that, if p is a prime not dividing \mathfrak{A} , then the zero set in $\overline{\mathbb{F}}_p^n$ of the polynomials $G_i \bmod p$, $i = 1, \dots, s$, consists of exactly κ distinct points.

Given two univariate polynomials $F_1, F_2 \in \mathbb{Z}[T]$, if their reductions $F_i \bmod p$, $i = 1, 2$, have a common zero in $\overline{\mathbb{F}}_p$, then their resultant $\text{Res}(F_1, F_2)$ is divisible by p . The following result refines this property for polynomials whose reduction modulo p has several common roots.

Theorem 3.4 ([GGIS09]). *Let A be a unique factorization domain with field of fractions K , $p \in A$ an irreducible element, and $F_1, F_2 \in A[T]$ two univariate polynomials whose reductions modulo p do not vanish identically and have at least N common roots in \overline{K} , counted with multiplicities. Then $p^N \mid \text{Res}(F_1, F_2)$.*

Indeed, for our application it is sufficient to use the result of [KS99, Lemma 5.3] taking only into account the number of different roots of the reductions of the polynomials F_i modulo p .

4. PROOFS OF THE MAIN RESULTS

In this section, we prove the results stated in §2. We start with Theorem 2.1 and its consequences.

Proof of Theorem 2.1. Fix $1 \leq \nu \leq r$ and $1 \leq j \leq s$. Given $0 \leq k \leq L - 1$, a point $\mathbf{t} \in \mathbb{C}^n$ verifies that

$$\mathbf{F}_\nu^{(L)}(\mathbf{a}_j, \mathbf{t}) = \mathbf{F}_\nu^{(k)}(\mathbf{a}_j, \mathbf{t})$$

if and only if it lies in the zero set of the ideal

$$I_{\nu,j,k} = \left(F_{\nu,i}^{(L)}(\mathbf{a}_j, \mathbf{T}) - F_{\nu,i}^{(k)}(\mathbf{a}_j, \mathbf{T}) : 1 \leq i \leq m \right) \subseteq \mathbb{Z}[\mathbf{T}].$$

Hence, $\#\text{Orb}_{\mathbf{F}_\nu, \mathbf{t}}(\mathbf{a}_j) \leq L$ if and only if \mathbf{t} lies in the zero set of the ideal $\prod_{k=0}^{L-1} I_{\nu,j,k}$.

For each $\nu = 1, \dots, r$, $\mathbf{i} \in \{1, \dots, m\}^L$ and $j = 1, \dots, s$, consider the polynomial

$$\Psi_{\nu, \mathbf{i}, j} = \prod_{k=0}^{L-1} \left(F_{\nu, i_{k+1}}^{(L)}(\mathbf{a}_j, \mathbf{T}) - F_{\nu, i_{k+1}}^{(k)}(\mathbf{a}_j, \mathbf{T}) \right) \in \mathbb{Z}[\mathbf{T}].$$

This gives a set of $rs m^L$ generators of the ideal

$$\sum_{\nu=1}^r \sum_{j=1}^s \prod_{k=0}^{L-1} I_{\nu,j,k} \subseteq \mathbb{Z}[\mathbf{T}].$$

Hence, for a point $\mathbf{t} \in \mathbb{C}^n$,

$$(4.1) \quad \max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_\nu, \mathbf{t}}(\mathbf{a}_j) \leq L$$

if and only if $\Psi_{\nu, \mathbf{i}, j}(\mathbf{t}) = 0$ for all ν , \mathbf{i} and j . Moreover, the set of such parameters \mathbf{t} is contained in the set of $\mathbf{t} \in \mathbb{C}^n$ such that $\mathbf{a}_j \in \text{PrePer}_{\mathbb{C}}(\mathbf{F}_\nu, \mathbf{t})$ for all ν and j . By hypothesis, this latter set is empty if $n = 0$, and finite if $n \geq 1$. Hence, the number of possible values of \mathbf{t} 's satisfying (4.1) is finite and bounded above by the constant κ .

For $\nu = 1, \dots, r$, consider the family of $m + n$ polynomials in $m + n$ variables given by

$$\mathbf{R}_\nu = (\mathbf{F}_\nu, \mathbf{T}) \in \mathbb{Z}[\mathbf{X}, \mathbf{T}]^{m+n}.$$

For $k \geq 0$, we have that $\mathbf{R}_\nu^{(k)} = (\mathbf{F}_\nu^{(k)}, \mathbf{T})$. Hence, the k -th iteration of the system \mathbf{F}_ν with respect to the variables \mathbf{X} can be recovered from the first m coordinate

polynomials of the k -th iteration of the system \mathbf{R}_ν . Applying Lemma 3.2 to \mathbf{R}_ν , we deduce that $\deg \mathbf{F}_\nu^{(k)} \leq d^k$ and

$$h(\mathbf{F}_\nu^{(k)}) \leq h \frac{d^k - 1}{d - 1} + d(d + 1) \frac{d^{k-1} - 1}{d - 1} \log(m + n + 1) \ll_{m,n,r,s,h} d^k.$$

By Lemma 3.1, for all ν, \mathbf{i}, j ,

$$(4.2) \quad \deg \Psi_{\nu, \mathbf{i}, j} \leq Ld^L \quad \text{and} \quad h(\Psi_{\nu, \mathbf{i}, j}) \ll_{m,n,r,s,h} Ld^L.$$

When $n = 0$, the polynomials $\Psi_{\nu, \mathbf{i}, j}$ are constant. As in Remark 2.2, our hypothesis that there is no $\mathbf{t} \in \mathbb{C}^0 = \{0\}$ satisfying (4.1) implies that there exist ν_0 and j_0 such that $\mathbf{a}_{j_0} \notin \text{PrePer}_{\mathbb{C}}(\mathbf{F}_{\nu_0, 0})$, and thus $\Psi_{\nu_0, \mathbf{i}, j_0} \neq 0$ for all \mathbf{i} . In this case we take $\mathfrak{A}_L = \gcd\{\Psi_{\nu_0, \mathbf{i}, j_0} : \mathbf{i} \in \{1, \dots, m\}^L\}$.

When $n \geq 1$, we set \mathfrak{A}_L for the positive integer given by Theorem 3.3 applied to this family of polynomials, which satisfies

$$\begin{aligned} \log \mathfrak{A}_L &\leq (11n + 4)(Ld^L)^{3n+1} Ld^L + (55n + 99) \log((2n + 5)(rsm^L)) (Ld^L)^{3n+2} \\ &\ll_{m,n,r,s,h} L^{3n+3} d^{(3n+2)L}. \end{aligned}$$

In both cases, for every prime $p \nmid \mathfrak{A}_L$, the system of equations

$$\Psi_{\nu, \mathbf{i}, j}(\mathbf{a}_j \bmod p, \mathbf{t}) = 0$$

has at most κ solutions $\mathbf{t} \in \overline{\mathbb{F}}_p^n$. Similarly as before, this is equivalent to the statement that

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu, \mathbf{t}}}(\mathbf{a}_j \bmod p) > L,$$

for all but at most κ values of $\mathbf{t} \in \overline{\mathbb{F}}_p^n$, which proves the theorem. \square

Proof of Corollary 2.3. Theorem 2.1 applied with $L = \lfloor \varepsilon \log \log p \rfloor$ implies there is a positive integer \mathfrak{A}_L with

$$(4.3) \quad \log \mathfrak{A}_L \ll_{m,n,r,s,h} \begin{cases} (\varepsilon \log \log p)(\log p)^{\varepsilon \log d} & \text{if } n = 0, \\ (\varepsilon \log \log p)^{3n+3} (\log p)^{\varepsilon(3n+2) \log d} & \text{if } n \geq 1, \end{cases}$$

such that, for all $p \nmid \mathfrak{A}_L$, for all but at most κ values of $\mathbf{t} \in \overline{\mathbb{F}}_p^n$,

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu, \mathbf{t}}}(\mathbf{a}_j \bmod p) > \varepsilon \log \log p.$$

The bound (4.3) implies that there is a constant c , depending on the parameters m, n, r, s and h , such that $\mathfrak{A}_L < p$ for all $p \geq c$. For those primes p , we have that $p \nmid \mathfrak{A}_L$ and the result follows. \square

Proof of Corollary 2.4. Let $Q \geq 2$. Theorem 2.1 applied with $L = \lfloor \varepsilon \log Q \rfloor$ implies that there is an integer $\mathfrak{A}_L \geq 1$ with

$$(4.4) \quad \log \mathfrak{A}_L \ll_{m,n,r,s,h} \begin{cases} (\log Q) Q^{\varepsilon \log d} & \text{if } n = 0, \\ (\log Q)^{3n+3} Q^{\varepsilon(3n+2) \log d} & \text{if } n \geq 1, \end{cases}$$

such that, for all $p \leq Q$ with $p \nmid \mathfrak{A}_L$, for all but at most κ values of $\mathbf{t} \in \overline{\mathbb{F}}_p^n$,

$$(4.5) \quad \max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu, \mathbf{t}}}(\mathbf{a}_j \bmod p) > \varepsilon \log Q \geq \varepsilon \log p.$$

The divisibility $p \mid \mathfrak{A}_L$ is possible for at most $\log \mathfrak{A}_L / \log 2$ primes p . Hence, the bound (4.4) implies that the set of primes $p \leq Q$ not satisfying (4.5) is of size $\mathcal{O}_{m,n,r,s,h}(Q^\gamma)$ for an exponent $0 < \gamma < 1$. Hence, this subset of primes has natural density 0, and thus its complement has natural density 1, as stated. \square

We now treat polynomial systems depending on a single parameter T .

Proof of Theorem 2.7. For each $\nu = 1, \dots, r$, $\mathbf{i} \in \{1, \dots, m\}^L$ and $j = 1, \dots, s$, consider the polynomial

$$\Psi_{\nu, \mathbf{i}, j} = \prod_{k=0}^{L-1} \left(F_{\nu, \mathbf{i}_{k+1}}^{(L)}(\mathbf{a}_j, T) - F_{\nu, \mathbf{i}_{k+1}}^{(k)}(\mathbf{a}_j, T) \right) \in \mathbb{Z}[T].$$

As in the proof of Theorem 2.1, a point $t \in \mathbb{C}$ verifies that

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu, t}}(\mathbf{a}_j) \leq L$$

if and only if $\Psi_{\nu, \mathbf{i}, j}(t) = 0$ for all ν , \mathbf{i} and j . The set of such t is contained in the set (2.3) and, by the hypothesis on this latter, the number of such values of t is finite and bounded above by the constant κ .

As in (4.2), the number of such polynomials is $rs m^L$, and their degree and height are bounded by

$$(4.6) \quad \deg \Psi_{\nu, \mathbf{i}, j} \ll_{m,r,s,h} L d^L \quad \text{and} \quad h(\Psi_{\nu, \mathbf{i}, j}) \ll_{m,r,s,h} L d^L.$$

Let $H \in \mathbb{Z}[T]$ be a primitive polynomial that is a greatest common divisor in $\mathbb{Q}[T]$ of the polynomials $\Psi_{\nu, \mathbf{i}, j}$, and write

$$\Phi_0, \dots, \Phi_u$$

for the distinct nonzero polynomials of the form $\Phi_l = \Psi_{\nu, \mathbf{i}, j} / H$ for some ν, \mathbf{i} and j . We have that $u < rsm^L$, and we deduce from (4.6) and Lemma 3.1(2) that, for $l = 0, \dots, u$,

$$\deg \Phi_l \ll_{m,r,s,h} L d^L \quad \text{and} \quad h(\Phi_l) \ll_{m,r,s,h} L d^L.$$

Let $\mathbf{U} = (U_1, \dots, U_u)$ be a group of variables and set

$$\Phi = \sum_{l=1}^u U_l \Phi_l \quad \text{and} \quad R = \text{Res}(\Phi_0, \Phi) \in \mathbb{Z}[\mathbf{U}].$$

Since the polynomials Φ_l are coprime, it follows that Φ_0 and Φ are coprime. Moreover, Φ_0 is nonzero and so R is nonzero too. Using Sylvester's determinantal formula for the resultant and Lemma 3.1(2), we deduce that

$$\deg R \ll_{m,r,s,h} L^2 d^{2L} \quad \text{and} \quad h(R) \ll_{m,r,s,h} L^2 d^{2L},$$

and we set $\mathfrak{A}_L \in \mathbb{Z} \setminus \{0\}$ as any nonzero coefficient of this polynomial.

Let p be a prime and denote by $\Lambda_p \subseteq \overline{\mathbb{F}}_p$ the subset of $t \in \overline{\mathbb{F}}_p$ such that

$$\max_{\substack{1 \leq \nu \leq r \\ 1 \leq j \leq s}} \#\text{Orb}_{\mathbf{F}_{\nu, t}}(\mathbf{a}_j \bmod p) \leq L.$$

As before, this coincides with the zero set of the reductions of the polynomials $\Psi_{\nu, \mathbf{i}, j}$ modulo p . Let $\kappa + e_p$ be the cardinality of this set, with $e_p \in \mathbb{Z}$. We denote by $H_p, \Phi_p, \Phi_{l,p} \in \mathbb{F}_p[T]$ the reductions modulo p of $H, \Phi, \Phi_l \in \mathbb{Z}[T]$, $l = 0, \dots, u$, respectively.

If $t \in \Lambda_p$, then either $H_p(t) = 0$ or $\Phi_l(t) = 0$, $l = 0, \dots, u$. The number of zeros of H_p is bounded by $\deg H \leq \kappa$. The number of common zeros in $\overline{\mathbb{F}}_p$ of the polynomials $\Phi_{l,p}$ coincides with the number of common zeros in $\overline{\mathbb{F}}_p$ of $\Phi_{0,p}$ and Φ_p . By Theorem 3.4, this number is bounded above by $\text{ord}_p R$, the largest power of p dividing all coefficients of R . In turn, this is also bounded above by $\text{ord}_p \mathfrak{A}_L$ (which is the p -adic order of one of the non-zero coefficients of R). It follows that

$$\max\{0, e_p\} \leq \text{ord}_p \mathfrak{A}_L,$$

proving the result. \square

Proof of Corollary 2.8. Let $Q \geq 2$. Theorem 2.7 applied with $L = \lfloor \varepsilon \log Q \rfloor$ implies that there is an integer $\mathfrak{A}_L \geq 1$ such that

$$\log \mathfrak{A}_L \ll_{m,r,s,h} (\log Q)^2 Q^{2\varepsilon \log d}.$$

such that, for every p , for all but at most $\kappa + \text{ord}_p \mathfrak{A}_L$ values of $t \in \overline{\mathbb{F}}_p$,

$$\max_{\nu,j} \#\text{Orb}_{\mathbf{F}_{\nu,t}}(\mathbf{a}_j \bmod p) > \varepsilon \log Q \geq \varepsilon \log p.$$

The statement follows by taking any $2\varepsilon \log d < \gamma < 1$ and $c_p = \text{ord}_p \mathfrak{A}_L$. \square

ACKNOWLEDGEMENTS

During the preparation of this paper, Chang was partially supported by the NSF Grants DMS 1301608, D'Andrea by the Spanish MEC research project MTM2013-40775-P, Ostafe by the UNSW Vice Chancellor's Fellowship, Shparlinski by the ARC Grant DP140100118, and Sombra by the Spanish MINECO research project MTM2015-65361-P.

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>)
- [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.

- [GKNY17] D. Ghioca, H. Krieger, K. Nguyen and H. Ye, ‘The dynamical André-Oort conjecture: Unicritical polynomials’, *Duke Math. J.*, **166** (2017), 1–25.
- [GNT15] D. Ghioca, K. Nguyen and 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.
- [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.

CHANG: 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>

D’ANDREA: 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>

OSTAFE: 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>

SHPARLINSKI: 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>

SOMBRA: ICREA. PASSEIG LLUÍS COMPANYS 23, 08010 BARCELONA, SPAIN
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>