REDUCTION OF POLYNOMIAL DYNAMICAL SYSTEMS
MODULO PRIMES

S. S. ROUT

Abstract. We study the algebraic dynamical systems generated by triangular systems of rational functions and estimate the height growth of iterations generated by such systems. Further, using a result on the reduction modulo primes of systems of multivariate polynomials over the integers, we study the periodic points and the intersection of orbits of such dynamical systems over finite fields.

1. Introduction

Let $V \subset \mathbb{P}^N$ be a quasi-projective variety defined over a field $K$ and let

$$\Phi : V \rightarrow V$$

be an endomorphism. For any $m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, we denote by $\Phi^{(m)} = \Phi \circ \cdots \circ \Phi$ the $m$-th iteration of $\Phi$ with $\Phi^{(0)}$ denoting the identity map. For a given point $P \in V(K)$, the (forward) orbit of $P$ is the set

$$\text{Orb}_\Phi(P) = \{P, \Phi^{(1)}(P), \Phi^{(2)}(P), \ldots\}.$$ 

The point $P$ is called a periodic point for $\Phi$ if $\Phi^{(n)}(P) = P$ for some $n \geq 1$ and the smallest such $n$ is called the period of $P$. The point $P$ is called preperiodic if some iterate $\Phi^{(m)}(P)$ is periodic.

The area of algebraic dynamics was introduced by Northcott [9] and later, Silverman [11] greatly developed all aspects of the theory of algebraic dynamics. For a background of the dynamical systems associated with iterations, one can refer to [10, 11]. In [12], Silverman studied the orbit length for the reduction modulo a prime $p$ for any self morphism of a quasi-projective variety defined over a number field. Later, this result has been improved in [11]. Since then there have been many advances in the study of periodic points and period lengths in the reductions of orbits of dynamical systems modulo distinct primes $p$.

Motivated by the work of Towsley [13] on Hasse principle for periodic points, D’Andrea et. al., [3], using several tools from arithmetic geometry, have proved new results about the orbits of the reductions modulo a prime $p$ of algebraic

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

Key words and phrases. Algebraic dynamical system, arithmetic Nullstellensatz, reduction of systems of polynomials, orbit intersection, periodic point.
dynamical systems over $\mathbb{Q}$. Later in [2], Changa et. al., gives a lower bound for the orbit length of the reduction modulo primes of parametric polynomial dynamical systems defined over integers. As a by-product, their result recovers a result in [1] and slightly improves a result in [12].

The results in [3] depends on the growth of the degree and the height of the iterates. When this growth is slower than generic, one can expect stronger bounds. Although for a typical system an exponential degree growth is expected, there are rich families of multivariate polynomial systems with a much slower degree growth (see [4, 5, 6, 7]). For example, for triangular system of polynomials, it has been shown in [6] that degrees of the iterations of the polynomials in triangular system grow very slowly.

In this paper, we consider the following class of rational dynamical systems with slow degree growth.

Let

\[
F = (F_1, \ldots, F_n), \quad F_1, \ldots, F_n \in \mathbb{Q}(X)
\]

be a system of $n$ rational functions in $n$ variables $(X_1, \ldots, X_n)$ over $\mathbb{Q}$ where

\[
F_1(X_1, \ldots, X_n) = X_1^{e_1}G_1(X_2, \ldots, X_n) + H_1(X_2, \ldots, X_n)
\]

\[
\ldots
\]

\[
F_{n-1}(X_1, \ldots, X_n) = X_n^{e_{n-1}G_{n-1}(X_n) + H_{n-1}(X_n)}
\]

\[
F_n(X_1, \ldots, X_n) = g_nX_n^{e_n} + h_n,
\]

with $e_1, \ldots, e_n \in \{-1, 1\}$, $G_i, H_i \in \mathbb{Z}[X_{i+1}, \ldots, X_n], i = 1, \ldots, n-1$ and $g_n, h_n \in \mathbb{Z}, g_n \neq 0$. We define the iterations of the rational function $F_i$ as follows.

\[
G_i^{(\ell)}(X_{i+1}, \ldots, X_n) = G_i(F_i^{(\ell-1)}, \ldots, F_n^{(\ell-1)}),
\]

\[
H_i^{(\ell)}(X_{i+1}, \ldots, X_n) = H_i(F_i^{(\ell-1)}, \ldots, F_n^{(\ell-1)}).
\]

Our first main result in this paper gives a bound for the number of points of a given period in the reduction modulo $p$ of the algebraic dynamical system defined in (2). Also, we give a bound for the frequency of the points in an orbit of the reduction modulo $p$ of the algebraic dynamical systems defined in (2) lying in a given algebraic variety. To prove these results, we use a deep result from arithmetic geometry [3, Theorem 2.1].

### 2. Notation and Main Results

Let $X$ denotes the group of variables $(X_1, \ldots, X_n)$ so that $\mathbb{Z}[X]$ denotes the ring of polynomials $\mathbb{Z}[X_1, \ldots, X_n]$ and $\mathbb{Q}(X)$ denotes the field of rational functions $\mathbb{Q}(X_1, \ldots, X_n)$. Let $\overline{K}$ denote an algebraic closure of a field $K$ of characteristic zero.
For a polynomial $L \in \mathbb{Z}[X]$, we define its height as the logarithm of the maximum of the absolute values of its coefficients and denote it by $h(L)$. For a rational function $F \in \mathbb{Q}(X)$, we write $F = L/K$ with coprime $L, K \in \mathbb{Z}[X]$ and we define the degree and the height of $F$, respectively, as the maximum of the degrees and of the heights of $L$ and $K$, that is,

$$\deg F = \max\{\deg L, \deg K\} \quad \text{and} \quad h(F) = \max\{h(L), h(K)\}.$$ 

To give explicit formula for degree growth of the iterates of the system in (2), we impose the following conditions on the degrees of the polynomials $G_i$ and $H_i$ for $i = 1, \ldots , n - 1$ (see [6, 7]).

If $e_i = 1$, we assume that the polynomial $G_i$ has a unique leading monomial $X^{s_{i+1}} \cdots X^{s_i}$, that is

$$G_i = g_i X_{i+1}^{s_{i+1}} \cdots X_n^{s_n} + \tilde{G}_i,$$

where $g_i \in \mathbb{Z} \setminus \{0\}$ and $\tilde{G}_i \in \mathbb{Z}[X_{i+1}, \ldots , X_n]$ with

$$\deg_{X_j} \tilde{G}_i < s_{i,j}, \quad \deg_{X_j} H_i < s_{i,j}, \quad j = i + 1, \ldots , n. \quad (3)$$

If $e_i = -1$, we assume that the polynomial $H_i$ has a unique leading monomial $X^{s_{i+1}} \cdots X_n$, that is

$$H_i = h_i X_{i+1}^{s_{i+1}} \cdots X_n^{s_n} + \tilde{H}_i,$$

where $h_i \in \mathbb{Z} \setminus \{0\}$ and $\tilde{H}_i \in \mathbb{Z}[X_{i+1}, \ldots , X_n]$ with

$$\deg_{X_j} \tilde{H}_i < s_{i,j}, \quad \deg_{X_j} G_i < 2s_{i,j}, \quad j = i + 1, \ldots , n. \quad (4)$$

We define the orbit of a given point $w \in \overline{\mathbb{Q}}^n$ with respect to the system of rational functions in (1) as the set

$$(5) \quad \text{Orb}_F(w) = \{w_k \mid w_0 = w \quad \text{and} \quad w_k = F(w_{k-1}), \ k = 1, 2, \ldots \}.$$ 

If $w_k$ is a pole of $F$, then the orbit terminates and in this case $\text{Orb}_F(w)$ is a finite set. Further, given $k \geq 1$, we say that $w \in \overline{\mathbb{Q}}^n$ is $k$-periodic if the element $w_k$ exists in the orbit (5) and we have $w_k = w_0$. Further, we put

$$(6) \quad S(w) = \# \text{Orb}_F(w) \in \mathbb{N} \cup \{\infty\}.$$ 

Let $p \in \mathbb{Z}$ be a prime. For each prime $p$, set $F_i^{(m)} = F_i^{(m)} (\mod p)$. We define the reduction modulo $p$ of the iteration $F^{(m)}$ and denote this by

$$F_p^{(m)} = (F_{1,p}^{(m)}, \ldots , F_{n,p}^{(m)}) \in \mathbb{F}_p[X]^n.$$ 

Let $L = (L_1, \ldots , L_s) \in \mathbb{Z}[X]$ be a system of polynomials of degree at most $D$ and height at most $H$. We denote by $V$ the subvariety of the affine space $\mathbb{A}_D^n$ defined by this system of polynomials. For a prime $p$, we denote by $L_{i,p} \in \mathbb{F}_p[X]$ the reduction modulo $p$ of $L_i$ and by $V_p$ the subvariety of $\mathbb{A}_D^n_{\mathbb{F}_p}$ defined by the system $L_{i,p}, i = 1, \cdots , s$. 
Given the functions
\[ f, g : \mathbb{N} \to \mathbb{R} \]
the symbols \( f = O(g) \) and \( f \ll g \) both mean 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, say \( n, d, h \), we write \( f = O_{n, d, h}(g) \) and \( f \ll_{n, d, h} g \).

The following result is concerned with the number of points of a given period in the reduction modulo \( p \) of triangular systems of polynomials as in (1) with \( e_i = 1 \).

**Theorem 2.1.** Let \( F_1, \ldots, F_n \in \mathbb{Z}[X] \) be as in (2) with \( e_i = 1 \), satisfying the condition (3) such that \( s_{i,i+1} \neq 0, i = 1, \ldots, n - 1 \). Set
\[ d = \max_{j=1,\ldots,n} \deg F_j \quad \text{and} \quad h = \max_{j=1,\ldots,n} h(F_j). \]
Suppose that \( F = (F_1, \ldots, F_n) \) has finitely many periodic points of order \( k \) over \( \mathbb{C} \). Then there exists an integer \( B_1 \in \mathbb{N} \) satisfying
\[ \log B_1 \ll_{d,h,n} k^{n(3n-1)} \]
and such that if \( p \) is a prime number not dividing \( B_1 \), then the reduction of \( F \) modulo \( p \) has \( O_{d,h,n}(k^{n(n-1)/2}) \) periodic points of order \( k \).

In the following theorem, we study the same result as in Theorem 2.1 for system in (1) with \( e_i = -1 \).

**Theorem 2.2.** Let \( n \in \mathbb{N} \) with \( n \geq 2 \). For \( i = 1, \ldots, n \), let \( F_i \) be rational functions defined by (2) satisfying the condition (4) such that \( s_{i,i+1} \neq 0, i = 1, \ldots, n - 1 \) and \( e_i = -1 \) for \( i = 1, \ldots, n \). Set
\[ d = \max_{j=1,\ldots,n} \deg F_j \quad \text{and} \quad h = \max_{j=1,\ldots,n} h(F_j). \]
Suppose that \( F = (F_1, \ldots, F_n) \) has finitely many periodic points of order \( k \) over \( \mathbb{C} \). Then there exists an integer \( B_2 \in \mathbb{N} \) satisfying
\[ \log B_2 \ll_{d,h,n} k^{n(3n^2+8n+9)/2} \]
and such that if \( p \) is a prime number not dividing \( B_2 \), then the reduction of \( F \) modulo \( p \) has \( O_{d,h,n}(k^{2n^2}) \) periodic points of order \( k \).

Next we obtain an upper bound for the frequency of the orbit intersections of a rational function system. More generally, we bound the number of points in such an orbit that belong to a given algebraic variety.

For \( \ell \in \mathbb{N} \), let \( p \) be a prime such that the iterations \( F^{(j)} \) with \( j = 0, \ldots, \ell - 1 \) can be reduced modulo \( p \). Given a point \( w \in \mathbb{F}_p^m \), we define
\[ \mathcal{J}_w(F, V; p, \ell) = \{ m \in \{0, 1, \ldots, \ell - 1\} \mid F_p^{(m)}(w) \in V_p(\mathbb{F}_p) \}. \]
We say that the iterations of $F$ \textit{generically escape} $V$ if for every integer $k \geq 1$, the $k$-th iteration of $F$ is well defined and the set

$$\{ w \in \mathbb{C}^n \mid (w, F^{(k)}(w)) \in V(\mathbb{C}) \times V(\mathbb{C}) \}.$$ is finite.

**Theorem 2.3.** Let $n \in \mathbb{N}$ with $n \geq 2$. For $i = 1, \ldots, n$, let $F_i$ be rational functions defined by (2) satisfying the conditions (3) and (4) and such that $s_{i,i+1} \neq 0, i = 1, \ldots, n - 1$. Set

$$d = \max_{j=1,\ldots,n} \deg F_j \quad \text{and} \quad h = \max_{j=1,\ldots,n} h(F_j).$$

Let $V$ be the subvariety of $\mathbb{A}^n_\mathbb{Q}$ defined by the system of polynomials $(L_1, \ldots, L_s) \in \mathbb{Z}[X]$ of degree at most $D$ and height at most $H$. Assume that the iterations of $F$ generically escape $V$. Then, there is a constant $C > 0$ (depending on $D$, $H$, $d$, $h$, $n$, $s$) such that for any real $\epsilon > 0$ and $\ell \in \mathbb{N}$ with

$$\ell \geq \frac{n^6 D^{2s}}{\epsilon(n-1)s+2},$$ there exists $\mathcal{D} \in \mathbb{N}$ with

$$\log \mathcal{D} \leq C/\epsilon^{n(3n-1)}$$ such that if $p$ is a prime number not dividing $\mathcal{D}$, then for any $w \in \mathbb{F}_p^n$ with $S(w) \geq \ell$,

$$\# \mathcal{I}_w (F, V; p, \ell) \leq \epsilon \ell.$$

Next we obtain a better result for the problem of bounding the frequency of the points in an orbit lying in a given variety under a restrictive condition.

Let $F \in \mathbb{Q}[X]^n$ be a system of rational functions over $K$ and let $V \subseteq \mathbb{A}^n_{\mathbb{Q}}$ be an affine variety. The intersection of the orbit $F$ with $V$ is $L$-\textit{uniformly bounded} if there is a constant $L$ depending only on $F$ and $V$ such that for all initial values $w \in \mathbb{Q}^n$,

$$\# \{ m \in \mathbb{N} \mid w_m \in V(\overline{\mathbb{Q}}) \} \leq L,$$ where $w_m$ is defined in [3].

**Theorem 2.4.** Let $n \in \mathbb{N}$ with $n \geq 2$. For $i = 1, \ldots, n$, let $F_i$ be rational functions defined by (2) satisfying the conditions (3) and (4) and such that $s_{i,i+1} \neq 0, i = 1, \ldots, n - 1$. Set

$$d = \max_{j=1,\ldots,n} \deg F_j \quad \text{and} \quad h = \max_{j=1,\ldots,n} h(F_j).$$

Let $V$ be the subvariety of $\mathbb{A}^n_{\mathbb{Q}}$ defined by the system of polynomials $(L_1, \ldots, L_s) \in \mathbb{Z}[X]$ of degree at most $D$ and height at most $H$. Assume that the intersection of
orbits of $F$ with $V$ is $L$-uniformly bounded. There is a constant $C > 0$ (depending on $D, H, d, h, n, L, s$) such that for any real $\epsilon > 0$ there exists $C \in \mathbb{N}$ with
\[
\log C \leq \frac{C}{\epsilon(n-1)(3n+2)+(n+L+2)}
\]
such that if $p$ is a prime number not dividing $C$, then for any integer
\[
\ell \geq \frac{2L}{\epsilon} + 1
\]
and for any initial point $w \in \mathbb{F}_p^n$ with $S(w) \geq \ell$, we have
\[
\#J_w(F; V; p, \ell) \leq \epsilon \ell.
\]

3. Preliminaries

In this section, we gather some bounds on the heights and the degrees of triangular polynomial systems. We start with bounds for the heights of sums and products of polynomials, which follows from [8, Lemma 1.2].

**Lemma 3.1.** Let $K_1, \ldots, K_t \in \mathbb{Z}[X]$. Then
\[
(1) \quad h\left(\sum_{i=1}^t K_i\right) \leq \max_{1 \leq i \leq t} h(K_i) + \log t;
\]
\[
(2) \quad -2\log(n+1) \sum_{i=1}^t \deg K_i \leq h\left(\prod_{i=1}^t K_i\right) - \sum_{i=1}^t h(K_i) \leq \log(n+1) \sum_{i=1}^t \deg K_i.
\]

The following is the standard bound for the degree and height of the composition of polynomials with integer coefficients (see [8, Lemma 1.2(1.c)]).

**Lemma 3.2.** Let $L \in \mathbb{Z}[Y_1, \ldots, Y_t], K_1, \ldots, K_t \in \mathbb{Z}[X]$. Set
\[
d = \max_{i=1, \ldots, t} \deg K_i \quad \text{and} \quad h = \max_{i=1, \ldots, t} h(K_i).
\]
Then,
\[
\deg(L(K_1, \ldots, K_t)) \leq d\deg L
\]
\[
h(L(K_1, \ldots, K_t)) \leq h(L) + \deg L(h + \log(t + 1) + d\log(n + 1)).
\]

The following is an extension of Lemma 3.2 to the composition of rational functions (see [3]).

**Lemma 3.3.** Let $L, K_1, \ldots, K_n \in \mathbb{Q}[X]$ such that the composition $L(K_1, \ldots, K_n)$ is well defined. Set
\[
d = \max_{i=1, \ldots, n} \deg K_i \quad \text{and} \quad h = \max_{i=1, \ldots, n} h(K_i).
\]
Then,
\[
\deg(L(K_1, \ldots, K_n)) \leq dn\deg L
\]
\[
h(L(K_1, \ldots, K_n)) \leq h(L) + h\deg L + (3dn + 1)\deg L \log(n + 1).
The following lemma gives the degree growth of the iterations of function defined by (2) (see [7, Theorem 2]).

**Lemma 3.4.** Let \( F_1, \ldots, F_n \) be rational functions defined by (2) satisfying the conditions (3) and (4) and such that \( s_{i,i+1} \neq 0, i = 1, \ldots, n - 1 \). Then degrees of the iterations of \( F_1, \ldots, F_n \) grow as follows

\[
\begin{align*}
\deg F_i^{(k)} &= 1 - \frac{1}{(n-i)!} k^{n-i} s_{i,i+1} \cdots s_{n-1,n} + \psi_i(k), \quad i = 1, \ldots, n - 1, \\
\deg F_n^{(k)} &= 1
\end{align*}
\]

where \( \psi_i(T) \in \mathbb{Q}[T] \) is a polynomial of degree \( \deg \psi_i < n-i \).

**Lemma 3.5.** For \( i = 1, \ldots, n \), let \( G_i \in \mathbb{Z}[X_i, X_{i+1}, \ldots, X_n] \) be a triangular system of polynomials with a unique leading monomial of the form \( X_{i+i+1} \cdots X_{n,n} \) and \( F_i \) as in (2). Set

\[
\begin{align*}
d &= \max_{i=1,\ldots,n} \deg F_i, \quad \text{and} \quad h = \max_{i=1,\ldots,n} h(F_i).
\end{align*}
\]

The height of the iterations of \( G_1, \ldots, G_n \) for \( k \geq 2 \) grow as follow:

\[
h(G_i^{(k)}) \leq \left( \sum_{j=1}^{k-1} \deg G_j^{(j)} \right) (h + \log(n-i)(n+1)^d) + h.
\]

Moreover, for any positive integer \( k \geq 2 \) and \( 1 \leq i \leq n \),

\[
h(G_i^{(k)}) \ll_{h,d,n} k^{n-i+1}.
\]

**Proof.** The inequality (7) for the height follows by induction on the number of iterates \( k \). We set for any \( k \geq 1 \) and \( 1 \leq i \leq n \)

\[
d_i,k = \deg G_i^{(k)}, \quad h_{i,k} = h \left( G_i^{(k)} \right).
\]

For \( k = 2 \), we have \( h(G_i^{(2)}) = G_i(F_{i+1}^{(1)}, \ldots, F_n^{(1)}) \). Now applying Lemma 3.2 to this,

\[
h(G_i^{(2)}) = h(G_i) + \deg(G_i)(h + \log(n-i) + d \log(n+1))
\]

\[
= h_{i,1} + d_{i,1}(h + \log(n-i) + d \log(n+1))
\]

\[
\leq (d_{i,1} + 1)h + d_{i,1} \log(n-i) + dd_{i,1} \log(n+1).
\]

Thus, the inequality (7) is true for \( k = 2 \). Now assume that inequality (7) is true for the first \( k-1 \) iterates. Applying Lemma 3.2 to the polynomial

\[
G_i^{(k)} = G_i^{(k-1)}(F_{i+1}, \ldots, F_n),
\]
\[
\begin{align*}
  h(G_i^{(k)}) &= h(G_i^{(k-1)}) + \deg(G_i^{(k-1)})(h + \log(n - i) + d \log(n + 1)) \\
  &\leq \left( \sum_{j=1}^{k-2} \deg G_i^{(j)} \right) (h + \log(n - i)(n + 1)^d) + h \\
  &\quad + d_{i,k-1}(h + \log(n - i) + d \log(n + 1)).
\end{align*}
\]
This proves inequality (7). Now from (7) and Lemma 3.4, we have
\[
  h(G_i^{(k)}) \leq \left( \sum_{j=1}^{k-1} \deg G_i^{(j)} \right) (h + \log(n - i)(n + 1)^d) + h
\]
\[
  = \left( \sum_{j=1}^{k-1} \deg G_i \left( F_{i+1}^{(j-1)}, \ldots, F_n^{(j-1)} \right) \right) (h + \log(n - i)(n + 1)^d) + h
\]
\[
  = \left( \sum_{j=1}^{k-1} \deg \left( (F_{i+1}^{(j-1)})^{s_{i,i+1}} \cdots (F_n^{(j-1)})^{s_{i,n}} \right) \right) (h + \log(n - i)(n + 1)^d) + h
\]
\[
  = \left( \sum_{j=1}^{k-1} \left( \frac{1}{(n - i - 1)!} (j - 1)^{n-i-1} s_{i,i+1} \cdots s_{n-1,n} + \cdots + (j - 1) s_{i,n} s_{n-1,n} + 1) \right) \right) \times (h + \log(n - i)(n + 1)^d) + h \ll_{h,d,n} k^{n-i+1}.
\]
This completes the proof. \(\square\)

Let us define the sets
\[
  I_+ = \{1 \leq i \leq n \mid e_i = \pm 1\}, \quad I_- = \{1 \leq i \leq n \mid e_i = -1\}.
\]

**Lemma 3.6.** Let \(F_1, \ldots, F_n\) be rational functions defined by (2) satisfying the conditions (3) and (4) and such that \(s_{i,i+1} \neq 0, i = 1, \ldots, n - 1\). Then height of the iterations of \(F_1, \ldots, F_n\) grow as follows:
\[
  h(F_i^{(k)}) \leq (k + 1) \deg(F_i^{(k)}) \log(n + 1) + \sum_{j=1}^{k} h(G_i^{(j)}) + \log 2
\]
for every \(i \in I_+\) and for every \(i \in I_-\)
\[
  h(F_i^{(k)}) \leq (k + 1) \deg(F_i^{(k)}) \log(n + 1) + \sum_{j=1}^{k} h(H_i^{(j)}) + (k + 1) \log 2.
\]
Moreover,
\[
  h(F_i^{(k)}) \ll_{d,h,n} k^{n-i+2}.
\]
Proof. First we prove the case when \( i \in I_+ \). The explicit structure of the iterations of the rational functions \( F_i \) are given in [7]. By [7, Lemma 2], we have

\[
F_i^k = \begin{cases} 
X_iG_{i,k} + H_{i,k}, & \text{for } i < n \\
g_n^kX_n + (g_n^{k-1} + \cdots + g_n + 1)h_n & \text{for } i = n,
\end{cases}
\]

where

\[
G_{i,k} = G_iG_{i}^{(2)} \cdots G_{i}^{(k)},
H_{i,k} = H_iG_{i}^{(2)} \cdots G_{i}^{(k)} + H_i^{(2)}G_{i}^{(3)} \cdots G_{i}^{(k)} + \cdots + H_i^{(k-1)}G_{i}^{(k)} + H_i^{(k)}.
\]

Applying Lemma 3.1 in equation (9) for \( i < n \),

\[
h(F_i^k) \leq h(X_iG_{i,k}) + \log 2 = h(X_iG_{i}^{(2)} \cdots G_{i}^{(k)}) + \log 2
\]

\[
\leq \deg(X_iG_{i}^{(2)} \cdots G_{i}^{(k)}) \log(n + 1) + \sum_{j=1}^{k} h(G_{i}^{(j)}) + h(X_i) + \log 2
\]

\[
\leq (k + 1) \deg(F_i^{(k)}) \log(n + 1) + \sum_{j=1}^{k} h(G_{i}^{(j)}) + \log 2.
\]

Again using Lemma 3.1 in (9) for \( i = n \),

\[
h(F_n^{(k)}) = h(g_n^kX_n + (g_n^{k-1} + \cdots + g_n + 1)h_n) \leq h(g_n^kX_n) + \log(k + 1)
\]

\[
\leq \log(g_n^k(n + 1)(k + 1)).
\]

Now consider the case \( i \in I_- \) and \( i < n \). In this case, by [7, Lemma 2], we have

\[
F_i^{(k)} = \frac{X_iR_{i,k} + S_{i,k}}{X_iR_{i,k-1} + S_{i,k-1}},
\]

where \( R_{i,k}, S_{i,k} \) are defined by the recurrence relations

\[
R_{i,k} = G_{i}^{(k)}R_{i,k-2} + H_{i}^{(k)}R_{i,k-1}, \quad S_{i,k} = G_{i}^{(k)}S_{i,k-2} + H_{i}^{(k)}S_{i,k-1}
\]

for \( k \geq 1 \) with the initial rational functions

\[
R_{i,0} = 1, S_{i,0} = 0, R_{i,1} = H_i, S_{i,1} = G_i.
\]

From Lemma 3.1 and (10),

\[
h(F_i^{(k)}) \leq \max\{h(X_iR_{i,k} + S_{i,k}), h(X_iR_{i,k-1} + S_{i,k-1})\}
\]

\[
\leq h(X_iR_{i,k}) + \log 2
\]

\[
\leq \deg(X_iR_{i,k}) \log(n + 1) + h(R_{i,k}) + h(X_i) + \log 2.
\]
Applying Lemma 3.1 in (11), one can inductively show that

\[(13) \quad h(R_{i,k}) \leq (\deg(R_{i,0} \cdots R_{i,k})) \log(n+1) + \sum_{j=1}^{k} h(H_{i}^{(j)}) + k \log 2\]

Thus, for \(i \in I_−\) and \(i < n\), from (12) and (13) we conclude

\[h(F_{i}^k) \leq (k+1) \deg\left(F_{i}^{(k)}\right) \log(n+1) + \sum_{j=1}^{k} h\left(H_{i}^{(j)}\right) + h(X_i) + (k+1) \log 2.\]

For the case \(e_{n} = -1\), we have

\[F_{n}^{(k)} = \left(\begin{array}{c}
(A_{1,k})_{1,1}X_{n} + (A_{1,k})_{1,2} \\
(A_{2,k})_{2,1}X_{n} + (A_{2,k})_{2,2}
\end{array}\right), \text{ where } A_{k} = \left(\begin{array}{cc}
h_{n} & g_{n} \\
1 & 0
\end{array}\right) = \left(\begin{array}{cc}
(A_{1,k})_{1,1} & (A_{1,k})_{1,2} \\
(A_{2,k})_{2,1} & (A_{2,k})_{2,2}
\end{array}\right).\]

One can observe that the entries of the matrix \(A_{k}\) are polynomials in the integer \(h_{n}\) and \(g_{n}\). Hence

\[h(F_{i}^k) \leq \max\left\{ h\left((A_{1,k})_{1,1}X_{n} + (A_{1,k})_{1,2}\right), h\left((A_{2,k})_{2,1}X_{n} + (A_{2,k})_{2,2}\right)\right\}\]

\[\leq h\left((A_{1,k})_{1,1}X_{n}\right) + h((A_{1,k})_{1,2}) + \log 2\]

\[\leq h\left((A_{1,k})_{1,1}\right) + h\left((A_{1,k})_{1,2}\right) + \log(2(n+1)) \leq \log(h_{n}(k+1)(n+1)).\]

This completes the estimates of \(h(F_{i}^k)\) for \(i \in I_−\) and \(i \leq n\). Also,

\[\sum_{j=0}^{k} j^{n-i+1} = \frac{1}{n-i+2} \left( B_{n-i+2}(k+1) - B_{n-i+2}(0) \right),\]

where \(B_{n-i+2}\) is the Bernoulli polynomial of degree \(n-i+2\) with leading coefficient equal to 1. Thus, from Lemma 3.5, the height of the \(k\)-th iteration of \(F_{i}\) is at most

\[h\left(F_{i}^{(k)}\right) \ll_{d,h,n} k^{n-i+2}.\]

The following result is on the reduction modulo primes of systems of multivariate polynomials over the integers, whose proof relies on the arithmetic Nullstellensatz (see [3, Theorem 2.1]).

**Lemma 3.7.** Let \(H_{1}, \ldots, H_{s} \in \mathbb{Z}[\mathbf{X}]\) be polynomials of degree at most \(d \geq 2\) and height at most \(h\), whose zero set in \(\mathbb{C}^{n}\) has a finite number \(T\) distinct points. Then there is an integer \(\mathfrak{A} \geq 1\) with

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

such that if \(p\) is a prime number not dividing \(\mathfrak{A}\), then the zero set in \(\mathbb{F}_{p}^{s}\) of the system of polynomials \(H_{i}(\mod p), i = 1, \ldots, s\) consists of exactly \(T\) distinct points.

We also need the following combinatorial result [3].
Lemma 3.8. Let $2 \leq M \leq N/2$. For any sequence
\[0 \leq n_1 < \cdots < n_M \leq N,\]
there exists $r \leq 2N/(M - 1)$ such that $n_{i+1} - n_i = r$ for at least $(M - 1)^2/4N$ values of $i \in \{1, \ldots, M - 1\}$.

Now we are ready to prove our results. The proof is motivated by the ideas of D’Andrea et. al., [3].

4. Proof of Main Results

4.1. Proof of Theorem 2.1
Consider the system of equations
\[F_i^{(k)} - X_i = 0, \quad i = 1, \ldots, n.\]
The set of $k$-periodic points of $F$ coincides with the zero set
\[V_k = Z \left( F_1^{(k)} - X_1, \ldots, F_n^{(k)} - X_n \right),\]
For $i = 1, \ldots, n$,
\[\deg \left( F_i^{(k)} - X_i \right) = \frac{1}{(n - i)!}k^{n-i}(s_{i,i+1} \cdots s_{n-1,n}) + 1,\]
and
\[h \left( F_i^{(k)} - X_i \right) \leq \max \left\{ h \left( F_i^{(k)} \right), h(X_i) \right\} + \log 2 \ll d,h,n k^{n-i+2}.\]
Now apply Lemma 3.7 and derive
\[\log B_1 \leq C_1(n, d, h)(k^{n-1})^{3n+1}k^{n+1} + C_2(n, d, h)(k^{n-1})^{3n+2} \ll d,h,n k^{n(3n-1)}.\]
Suppose $T_k$ is the number of points of $V_k$ over $\mathbb{C}$ and this equal to the number of periodic points of order $k$ of $F$ over $\mathbb{C}$. By Bezout’s theorem,
\[T_k \leq 2 \prod_{i=1}^{n} k^{n-i} \ll_{n,d,h} k^{n(n-1)/2}.\]
This completes the proof.

4.2. Proof of Theorem 2.2
By equation (10), the iterates of the system of rational functions $F$ is given by
\[F_i^{(k)} = \frac{X_i R_{i,k} + S_{i,k}}{X_i R_{i,k-1} + S_{i,k-1}} =: \frac{\Gamma_{i,k}}{\Psi_{i,k}}\]
with $\Psi_{i,k} \neq 0$ and consider the system of equations
\[\Gamma_{i,k} - X_i \Psi_{i,k} = 0, \quad i = 1, \ldots, n.\]
To extract the poles of $F_i^{(j)}, j \leq k$ from the solutions of the system, we introduce a new variable $X_0$. Now the set of $k$-periodic points of $F$ coincides with the zero set

$$V_k = Z \left( \Gamma_{1,k} - X_1 \Psi_{1,k}, \ldots, \Gamma_{n,k} - X_n \Psi_{n,k}, 1 - X_0 \prod_{i=1}^{n} \prod_{j=1}^{k} \Psi_{i,j} \right).$$

For $i = 1, \ldots, n$

$$\deg(\Gamma_{i,k} - X_i \Psi_{i,k}) \leq k^{n-i} + 1 \leq C_3(n, d)k^{n-i}$$

and

$$h(\Gamma_{i,k} - X_i \Psi_{i,k}) \leq h(F_i^{(k)}) + \log 2 \leq C_4(n, d, h)k^{n-i+2}.$$

Now

$$\deg \left( X_0 \prod_{i=1}^{n} \prod_{j=1}^{k} \Psi_{i,j} \right) \leq 1 + \sum_{i=1}^{n} \sum_{j=1}^{k} j^{n-i} \leq C_5(n, d, h)k^{n(n+1)/2}.$$

By Lemma 3.3

$$h \left( X_0 \prod_{i=1}^{n} \prod_{j=1}^{k} \Psi_{i,j} \right) = h \left( \prod_{i=1}^{n} \prod_{j=1}^{k} \Psi_{i,j} \right)$$

$$\leq \sum_{i=1}^{n} \sum_{j=1}^{k} h(\Psi_{i,j}) + \log(n+1) \left( \sum_{i=1}^{n} \sum_{j=1}^{k} \deg \Psi_{i,j} \right)$$

$$\leq \sum_{i=1}^{n} \sum_{j=1}^{k} j^{n-i+2} + C_5 \log(n+1)nk^{n(n+1)/2} \leq C_6(n, d, h)k^{n(n+5)/2}.$$

We apply Lemma 3.7 with $n + 1$ polynomials and $n + 1$ variables,

$$\log \mathfrak{B}_2 \ll_{n, d, h} k^{(n+1)/2} \left( k^{n(n+1)/2} \right)^{3(n+1)+1} + (k^{n(n+1)/2})^{3(n+1)+2}$$

$$\ll_{d, h, n} k^{n(3n^2+8n+9)/2}.$$

Again by Bezout’s theorem,

$$T_k \leq 2k^{n(n+1)/2} \prod_{i=1}^{n} k^{n-i} \ll_{n, d, h} k^{n^2}.$$

This completes the proof of theorem. □
4.3. **Proof of Theorem 2.3.** Let \( p \) be a prime and let \( L = (L_1, \ldots, L_s) \in \mathbb{Z}[X] \) be a system of polynomials of degree at most \( D \) and height at most \( H \). We denote by \( V \) the subvariety of the affine space \( \mathbb{A}^n_{\mathbb{Q}} \) defined by this system of polynomials. We also denote the reduction modulo \( p \) of the iteration \( F^{(m)} \) and \( V \) by \( F^{(m)}_p \) and \( V_p \), respectively. Here we fix an initial point \( w \in \mathbb{F}_p^m \) and let

\[
A = \# \left\{ m \in \{0, 1, \ldots, \ell - 1\} \mid F^{(m)}_p(w) \in V_p(\mathbb{F}_p) \right\}.
\]

Suppose that

\[
A > \varepsilon \ell \geq 2.
\]

Take \( \gamma \leq 2\ell/(A - 1) \) and let \( B \) be number of \( m \in \{0, 1, \ldots, \ell - 1\} \) with

\[
F^{(m)}_p(w) \in V_p \quad \text{and} \quad F^{(m+\gamma)}_p(w) = F^{(\gamma)}_p(F^{(m)}_p(w)) \in V_p.
\]

By Lemma 3.8

\[
B \geq \left(\frac{A - 1}{2}\right) \gg \varepsilon^2 \ell\]

and hence we have \( \gamma \ll 1/\varepsilon \).

Since the iterations generically escape \( V \), the set \( \{ u \in V \mid F^{(\gamma)}(u) \in V \} \) is finite and this set is defined by the following 2s equations

\[
L_j(X) = L_j(F^{(\gamma)}(X)) = 0, \quad j = 1, \ldots, s.
\]

By Lemma 3.3 and 3.4 we have

\[
\deg L_j(F^{(\gamma)}) \leq Dn\gamma^{n-1}
\]

and from Bézout’s theorem

\[
\# \{ u \in V \mid F^{(\gamma)}(u) \in V \} \leq D^s(Dn\gamma^{n-1})^s \ll \frac{nD^{2s}}{\epsilon(n-1)^s}.
\]

From Lemma 3.6 we have

\[
h(F^{(\gamma)}) \ll d,h,n, \gamma^{n-i+2}
\]

and hence by Lemma 3.3

\[
h(L_j(F^{(\gamma)})) \leq H + D\gamma^{n+1} + (3Dn\gamma^{n-1} + 1)D \log(n + 1) \ll d,h,n, Dn\gamma^{n+1}.
\]

Here the degree and height of 2s polynomials in (19) are bounded by \( Dn\gamma^{n-1} \) and \( Dn\gamma^{n+1} \) respectively. By Lemma 3.7 there is a positive integer \( \mathfrak{D} \) with

\[
\log \mathfrak{D} \leq (11n + 4)(Dn\gamma^{n-1})^{3n+1}(Dn\gamma^{n+1})
\]

\[
+ (55n + 99) \log((2n + 5)s)(Dn\gamma^{n-1})^{3n+2} \leq \frac{C_7}{\epsilon n(3n-1)}
\]

such that if \( p \nmid \mathfrak{D} \), then

\[
\# \{ u \in V \mid F^{(\gamma)}(u) \in V \} = \# \{ u \in V_p \mid F^{(\gamma)}_p(u) \in V_p \}.
\]
Since \( S(w) \geq \ell \), the points \( F^{(m)}_p(w) \), \( m = 0, \ldots, \ell - 1 \) are pairwise distinct. Hence,
\[
B \leq \# \{ u \in V_p \mid F^{(\gamma)}_p(u) \in V_p \}.
\]
From (18) and (20), we have
\[
\epsilon^2 \ell \leq \frac{n^s D^{2s}}{\epsilon^{(n-1)s}}.
\]
This is a contradiction as \( \ell > \frac{n^s D^{2s}}{\epsilon^{(n-1)s}} \). Thus, \( A \leq \epsilon \ell \) and this completes the proof of theorem □.

4.4. Proof of Theorem 2.4. Set
\[
\beta = \left\lceil \frac{2L}{\epsilon} \right\rceil + 1;
\]
thus \( \ell \geq \beta \). For each set \( B \subseteq \{0, \ldots, \beta - 1\} \) of cardinality \( \#B = L + 1 \), we consider the system of equations
\[
L_j \left( F^{(k)} \right) = 0, \quad k \in B, \quad j = 1, \ldots, s.
\]
Since \( k \in B \), we have \( k \leq \beta - 1 \). By Lemma 3.3 and 3.4,
\[
\deg L_j \left( F^{(k)} \right) \leq k^{n-1} D n \leq (\beta - 1)^{n-1} D n.
\]
Again, by Lemma 3.3 and Lemma 3.6 we have
\[
h \left( L_j \left( F^{(k)} \right) \right) \leq H + D k^{n+1} + (3 n k^{n-1} + 1) D \log(n + 1) \ll_{H,n} D(\beta - 1)^{n+1}.
\]
Since the intersection of orbits of \( F \) with \( V \) is \( L \)-uniformly bounded and \( k \in B \), the system of equations in (21) has no common solution \( w \in \overline{Q}^n \). By Lemma 3.7 there exists \( C_B \in \mathbb{N} \) with
\[
\log C_B \leq (11n + 4)(Dn(\beta - 1)^n D(\beta - 1)^n + 1) D \log(n + 1) \ll_{H,n} D(\beta - 1)^{n+1}.
\]
\[
\leq C_8(Dn(\beta - 1)^n D(\beta - 1)^n)^{3n+2}(\beta - 1)^{n+1}.
\]
such that if \( p \) is a prime and \( p \nmid C_B \), then the reduction modulo \( p \) of the system of equations (21) has no solutions in \( \mathbb{F}_p^n \).

Now set
\[
\mathcal{E} = \prod_{B \subseteq \{0, \ldots, \beta - 1\} \atop \#B = L + 1} \mathcal{C}_B
\]
and hence
\[
\log \mathcal{E} \ll_{D,d,h,H,n,L} \left( \frac{\beta}{L + 1} \right)^{3n+2}(\beta - 1)^{n+1}
\]
\[
\leq \frac{C_9(D, d, h, H, n, L, s)}{\epsilon^{(n-1)(3n+2)+(n+L+2)}}.
\]
Let $p$ be a prime with $p \nmid C$. Suppose that for some $u \in \mathbb{F}_p^d$ there are at least $\ell \ell$ values of $n \in \{0, \ldots, \ell - 1\}$ with $F_p^{(n)}(u) \in V_p$. Since $\ell \geq \beta$, there is a non negative integer $i \leq \lfloor \ell / \beta \rfloor$ such that there are at least
\[
\frac{\ell \ell}{\lfloor \ell / \beta \rfloor + 1} \geq \frac{\epsilon \beta}{2} > L
\]
values of $n \in \{i \beta, \ldots, (i + 1) \beta - 1\}$ with $F_p^{(n)}(u) \in V_p$. Now consider $L + 1$ values $i \beta < i \beta + \delta_1 < \cdots < i \beta + \delta_{L+1} < (i + 1) \beta$.

Then for $j = 1, \ldots, s$ and $t = 1, \ldots, L + 1$,
\[
L_j \left( F_p^{(i \beta)} \left( F_p^{(i \beta)} \right) \right) = 0.
\]
Setting $w = F_p^{(i \beta)} \in \mathbb{F}_p^d$, then for all $j, t$
\[
L_j \left( F_p^{(\delta_k)} (w) \right) = 0.
\]
This implies that $p \nmid C_B$ with $B = \{\delta_1, \ldots, \delta_{L+1}\}$ which is a contradiction. This completes the proof of theorem \( \square \).

References

[1] A. Akbary and D. Ghioca, Periods of orbits modulo primes, J. Number Theory, 129 (2009) 2831-2842.
[2] M. Chang, C. D’Andrea, A. Ostafe, I. Shparlinski and M. Sombra, Orbits of polynomial dynamical systems modulo primes, Proc. Amer. Math. Soc. 146 (2018) 2015-2025.
[3] C. D’Andrea, A. Ostafe, I. Shparlinski and M. Sombra, Reduction modulo primes of systems of polynomial equations and algebraic dynamical systems, Trans. Amer. Math. Soc. 371 (2019) 1169-1198.
[4] D. Gómez-Pérez, A. Ostafe and I. Shparlinski, Algebraic entropy, automorphisms and sparsity of algebraic dynamical systems and pseudorandom number generators, Math. Comp., 83 (2014) 1535-1550.
[5] B. Hasselblatt and J. Propp, Degree-growth of monomial maps, Ergodic Theory Dynam. Systems, 27 (2007) 1375-1397.
[6] A. Ostafe and I. Shparlinski, On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators, Math. Comp., 79 (2010) 501-511.
[7] A. Ostafe and I. Shparlinski, Degree growth, linear independence and periods of class of rational dynamical systems, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol 574, Amer. Math. Soc., Providence, RI, 2012, pp.131-143.
[8] T. Krick, L.M. Pardo and M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Math. J. 109 (2001) 521-598.
[9] D.G. Northcott, Periodic points on an algebraic variety, Ann. of Math. 51 (1950) 167–177.
[10] K. Schmidt, Dynamical systems of algebraic origin, Progress in Mathematics, vol 128, Birkhäuser Verlag, Basel, 1995.
[11] J. H. Silverman, The Arithmetic of Dynamical Systems, Springer, New York, 2007.
[12] J. H. Silverman, Variation of periods modulo $p$ in arithmetic dynamics, New York J. Math., 14 (2008) 601-616.
[13] A. Towsley, *A Hasse principle for periodic points*, Int. J. Number Theory 9(8) (2013), 2053-2068.

Sudhansu Sekhar Rout  
Institute of Mathematics & Applications,  
Andharua, Bhubaneswar-751 029,  
Odisha, India  
Email address: lbs.sudhansu@gmail.com