REDUCTIONS MODULO PRIMES OF SYSTEMS OF POLYNOMIAL EQUATIONS AND ALGEBRAIC DYNAMICAL SYSTEMS

CARLOS D'ANDREA, ALINA OSTAFE, IGOR E. SHPARLINSKI, AND MARTÍN SOMBRA

Abstract. We give bounds for the number and the size of the primes p such that a reduction modulo p of a system of multivariate polynomials over the integers with a finite number T of complex zeros, does not have exactly T zeros over the algebraic closure of the field with p elements.

We apply these bounds to study the periodic points and the intersection of orbits of algebraic dynamical systems over finite fields. In particular, we establish some links between these problems and the uniform dynamical Mordell–Lang conjecture.

1. Introduction

The goal of the paper is to extend the scope of application of algebraic geometric methods to algebraic dynamical systems, that is, to dynamical systems generated by iterations of rational functions.

Let

$$\boldsymbol{R} = (R_1, \dots, R_m), \qquad R_1, \dots, R_m \in \mathbb{Q}(\boldsymbol{X}),$$

be a system of m rational functions in m variables $\boldsymbol{X} = (X_1, \dots, X_m)$ over $\mathbb{Q}$. The iterations of this system of rational functions are given by

$$R_i^{(0)} = X_i \qquad \text{and} \qquad R_i^{(n)} = R_i(R_1^{(n-1)}, \dots, R_m^{(n-1)}) \tag{1.1}$$

for $i = 1, \dots, m$ and $n \geq 1$, as long as the compositions are well-defined. We refer to [AK09, Sch95, Sil07] for a background on the dynamical systems associated with these iterations.

For $i = 1, \dots, m$ and $n \geq 1$ write

$$R_i^{(n)} = \frac{F_{i,n}}{G_{i,n}} \tag{1.2}$$

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

Key words and phrases. Modular reduction of systems of polynomials, arithmetic Nullstellensatz, algebraic dynamical system, orbit length, orbit intersection.

D'Andrea was partially supported by the Spanish MEC research project MTM2013-40775-P, Ostafe by the UNSW Vice Chancellor's Fellowship, Shparlinski by the Australian Research Council Grants DP140100118 and DP170100786, and Sombra by the Spanish MINECO research projects MTM2012-38122-C03-02 and MTM2015-65361-P.

with coprime $F_{i,n}, G_{i,n} \in \mathbb{Z}[\boldsymbol{X}]$ and $G_{i,n} \neq 0$. Given a prime p such that $G_{i,j} \not\equiv 0 \pmod{p}$, $j = 1, \dots, n$, we can consider the reduction modulo p of the iteration (1.1). Recently, there have been many advances in the study of periodic points and period lengths in reductions of orbits of dynamical systems modulo distinct primes p [AG09, BGH+13, Jon08, RV09, Sil08]. However, many important questions remain widely open, including:

- the distribution of the period lengths,
- the number of periodic points,
- the number of common values in orbits of two distinct algebraic dynamical systems.

Furthermore, some of our motivation comes from the recently introduced idea of transferring the *Hasse principle* for periodic points and thus linking local and global periodicity properties [Tow13].

In this paper, we use several tools from arithmetic geometry to obtain new results about the orbits of the reductions modulo a prime p of algebraic dynamical systems. Our approach is based on a new result about the reduction modulo prime numbers of systems of multivariate polynomials over the integers. If the system has a finite number of solutions T over the complex numbers, then there exists a positive integer $\mathfrak{A}$ such that, for all prime numbers $p \nmid \mathfrak{A}$, the reduction modulo p of the system has also T solutions over $\overline{\mathbb{F}}_p$, the algebraic closure of the field with p elements. Here, using an arithmetic version of *Hilbert's Nullstellensatz* [DKS13, KPS01] and elimination theory, we give a bound, in terms of the degree and the height of the input polynomials, for the integer $\mathfrak{A}$ controlling the primes of bad reduction (Theorem 2.1). For $T = 0$, that is, for systems of polynomial equations without solutions over $\mathbb{C}$, this question has been previously adressed in [HMPS00, Koi96]. Indeed, the corresponding bound for the set of primes of bad reduction was a key step in Koiran's proof that, from the point of view of complexity theory, the satisfability problem for systems of polynomial equations lies in the polynomial hierarchy [Koi96].

As an immediate application of this result, in Theorems 4.2 and 4.3 we bound the number of points of given period in the reduction modulo p of an algebraic dynamical system. Also, combining Theorem 2.1 with some combinatorial arguments, we give in Theorem 5.3 a bound for the frequency of the points in an orbit of the reduction modulo p of an algebraic dynamical system lying in a given algebraic variety, or that coincide with a similar point coming from an orbit of another algebraic dynamical system (in Corollary 5.4).

We also use a different approach, based again on an explicit version of Hilbert's Nullstellensatz, to obtain in Theorem 6.2 better results for the problem of bounding the frequency of the points in an orbit lying in a given algebraic variety, under a different and apparently more restrictive condition.

Our bounds are uniform in the prime p, provided that p avoids a certain set of exceptions. In particular, our bounds for the number of k-periodic points can be viewed as distant relatives of the *Northcott theorem* for dynamical systems in [Sil07, Theorem 3.12], which bounds the number of pre-periodic points in algebraic dynamical systems over finite algebraic extensions of $\mathbb{Q}$. Here we restrict the length of the period, but instead we consider all k-periodic points over $\overline{\mathbb{F}}_p$.

From a computational point of view, the arithmetic Nullstellensätze in [DKS13, KPS01] are effective. Using this, one can show that the positive integers describing the set of exceptional primes in our results can be effectively computed.

Further applications of our results have been given in our subsequent paper with Chang [CDO+18].

Acknowledgements. We are grateful to Dragos Ghioca, Luis Miguel Pardo, Richard Pink, Thomas Tucker and Michael Zieve for many valuable discussions and comments, specially concerning the plausibility of the uniform boundedness assumption for the orbit intersections.

2. Modular Reduction of Systems of Polynomial Equations

2.1. **General notation.** Throughout this text, boldface letters denote finite sets or sequences of objects, where the type and number should be clear from the context. In particular, $\boldsymbol{X}$ denotes the group of variables $(X_1, \ldots, X_m)$, so that $\mathbb{Z}[\boldsymbol{X}]$ denotes the ring of polynomials $\mathbb{Z}[X_1, \ldots, X_m]$ and $\mathbb{Q}(\boldsymbol{X})$ the field of rational functions $\mathbb{Q}(X_1, \ldots, X_m)$.

We denote by $\mathbb{N}$ the set of positive integer numbers. Given functions

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

the symbols $f = O(g)$ and $f \ll g$ both mean that there is a constant $c \geq 0$ such that $|f(k)| \leq c\, g(k)$ for all $k \in \mathbb{N}$. To emphasize the dependence of the implied constant c on parameters, say m and s, we write $f = O_{m,s}(g)$ or $f \ll_{m,s} g$. We use the same convention for other parameters as well.

For a polynomial $F \in \mathbb{Z}[\boldsymbol{X}]$, we define its *height*, denoted by $\mathrm{h}(F)$, as the logarithm of the maximum of the absolute values of its coefficients. For a rational function $R \in \mathbb{Q}(\boldsymbol{X})$, we write $R = F/G$ with coprime $F, G \in \mathbb{Z}[\boldsymbol{X}]$ and we define the *degree* and the *height* of R respectively as the maximum of the degrees and of the heights of F and G, that is,

$$\deg R = \max\{\deg F, \deg G\} \qquad \text{and} \qquad \mathrm{h}(R) = \max\{\mathrm{h}(F), \mathrm{h}(G)\}.$$

Let K be a field and $\overline{K}$ its algebraic closure. Given a family of polynomials $G_1, \ldots, G_s \in K[\boldsymbol{X}]$, we denote by

$$V(G_1, \ldots, G_s) = \mathrm{Spec}\,(K[\boldsymbol{X}]/(G_1, \ldots, G_s)) \subset \mathbb{A}^m_K$$

its associated affine algebraic variety. We also denote by $Z(G_1,\dots,G_s)$ their zero set in $\overline{K}^m$, which coincides with the set of $\overline{K}$-valued points $V(G_1,\dots,G_s)(\overline{K})$.

Let

$$\boldsymbol{R} = (R_1,\dots,R_m), \qquad R_1,\dots,R_m \in K(\boldsymbol{X}) \tag{2.1}$$

be a system of m rational functions in m variables over K. For $n \ge 1$, we denote

$$\boldsymbol{R}^{(n)} = (R_1^{(n)},\dots,R_m^{(n)}),$$

as long as this iteration is well-defined as a rational function.

Given a point $\boldsymbol{w} \in \overline{K}^m$ we define its orbit with respect to the system of rational functions above as the set

$$\operatorname{Orb}_{\boldsymbol{R}}(\boldsymbol{w}) = \{\boldsymbol{w}_n \mid \text{with } \boldsymbol{w}_0 = \boldsymbol{w} \text{ and } \boldsymbol{w}_n = \boldsymbol{R}(\boldsymbol{w}_{n-1}),\ n = 1,2,\dots\}. \tag{2.2}$$

The orbit terminates if $\boldsymbol{w}_n$ is a pole of $\boldsymbol{R}$ and, in this case, $\operatorname{Orb}_{\boldsymbol{R}}(\boldsymbol{w})$ is a finite set.

If the point $\boldsymbol{w}_n$ in (2.2) is defined, then $\boldsymbol{w}_0$ is not a pole of $\boldsymbol{R}^{(n)}$ and $\boldsymbol{w}_n = \boldsymbol{R}^{(n)}(\boldsymbol{w}_0)$. However, the fact that the evaluation $\boldsymbol{R}^{(n)}(\boldsymbol{w}_0)$ is defined does not imply the existence of $\boldsymbol{w}_n$, since this latter point is defined if and only if all the previous points of the orbit (2.2) are defined and $\boldsymbol{w}_{n-1}$ is not a pole of $\boldsymbol{R}$. For instance, let $m = 1$ and $R(X) = 1/X$. Then $R^{(2)}(X) = X$ and we see that $R^{(2)}(0) = 0$, but $w_2 = R(R(0))$ is not defined as 0 is a pole for R. Clearly, for polynomial systems this distinction does not exist.

2.2. **Preserving the number of points.** The following is our main result concerning the reduction modulo prime numbers of systems of multivariate polynomials over the integers.

Theorem 2.1. *Let $m \ge 1$ and let $F_1,\dots,F_s \in \mathbb{Z}[\boldsymbol{X}]$ be a system of polynomials whose zero set in $\mathbb{C}^m$ has a finite number T of distinct points. Set*

$$d = \max_{i=1,\dots,s} \deg F_i \qquad \text{and} \qquad h = \max_{i=1,\dots,s} \mathrm{h}(F_i).$$

Then there exists $\mathfrak{A} \in \mathbb{N}$ satisfying

$$\log \mathfrak{A} \le C_1(m) d^{3m+1} h + C_2(m,s) d^{3m+2},$$

with

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

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

This result allows us to control the number and the height of the primes of bad reduction.

Corollary 2.2. *With notation as in Theorem 2.1, set* $\boldsymbol{F} = (F_1, \ldots, F_s)$ *and let* $S_{\boldsymbol{F}}$ *denote the set of prime numbers such that the number of zeros in* $\overline{\mathbb{F}}_p^m$ *of the system of polynomials* $F_i \pmod{p}$*,* $i = 1, \ldots, s$*, is different from* T*. Then*

$$\max\left\{\#S_{\boldsymbol{F}}, \max_{p\in S_{\boldsymbol{F}}} \log p\right\} \ll_{m,s} d^{3m+1}h + d^{3m+2}.$$

Remark 2.3. *In the interesting special case when* $s = m$*, one can get a slightly stronger version of Theorem 2.1, but of the same general shape.*

It is also very plausible that Theorem 2.1 admits a number of extensions such as zero-dimensional systems of polynomial equations on an equidimensional variety $X \subseteq \mathbb{A}^m_{\mathbb{C}}$ *instead of just on* $\mathbb{A}^m_{\mathbb{C}}$*. One can also obtain a bound taking into account the degree and the height of each individual polynomial* F_j*.*

2.3. **Preliminaries.** Besides the application of an arithmetic Nullstellensatz, the proof of Theorem 2.1 relies on elimination theory and on the basic properties of schemes over the integers. Hence, it is convenient to work using the language of algebraic geometry as in, for instance, [Liu02].

Let $F_1, \ldots, F_s \in \mathbb{Z}[\boldsymbol{X}]$ be a system of polynomials whose zero set in $\mathbb{C}^m$ has a finite number T of distinct points, as in the statement of Theorem 2.1. Denote by V the subvariety of the affine space $\mathbb{A}^m_{\mathbb{Q}} = \operatorname{Spec}(\mathbb{Q}[\boldsymbol{X}])$ defined by this system of polynomials. For each prime p, set

$$F_{i,p} \in \mathbb{F}_p[\boldsymbol{X}] \tag{2.3}$$

for the reduction modulo p of F_i, and by V_p the subvariety of $\mathbb{A}^m_{\mathbb{F}_p} = \operatorname{Spec}(\mathbb{F}_p[\boldsymbol{X}])$ defined by the system $F_{i,p}$, $i = 1, \ldots, s$.

Recall that, given a field extension $K \hookrightarrow L$ and a variety X over K, we denote by $X(L)$ the set of L-valued points of X. We have that

$$\mathbb{A}^m_{\mathbb{Q}}(\mathbb{C}) = \mathbb{C}^m \quad \text{and} \quad \mathbb{A}^m_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) = \overline{\mathbb{F}}_p^m,$$

and that the varieties $V(\mathbb{C})$ and $V_p(\overline{\mathbb{F}}_p)$ coincide with the zero sets $Z(F_1, \ldots, F_s)$ and $Z(F_{1,p}, \ldots, F_{s,p})$, respectively. Our aim is to give a bound for an integer $\mathfrak{A} \in \mathbb{N}$ such that, if $p \nmid \mathfrak{A}$, then $V_p(\overline{\mathbb{F}}_p)$ consists of T distinct points.

Let $\mathbb{A}^m_{\mathbb{Z}}$ and $\mathbb{P}^m_{\mathbb{Z}}$ be the affine space and the projective space over the integers, respectively. We denote by $\boldsymbol{Z} = \{Z_0, \ldots, Z_m\}$ the homogeneous coordinates of $\mathbb{P}^m_{\mathbb{Z}}$. Using the standard inclusion

$$\iota\colon \mathbb{A}^m_{\mathbb{Z}} \longrightarrow \mathbb{P}^m_{\mathbb{Z}} \quad , \quad (x_1, \ldots, x_m) \longmapsto (1 : x_1 : \ldots : x_m), \tag{2.4}$$

we identify $\mathbb{A}^m_{\mathbb{Z}}$ with the open subset of $\mathbb{P}^m_{\mathbb{Z}}$ given by the non-vanishing of Z_0. The coordinates of these spaces are then related by $X_i = Z_i/Z_0$.

Let $\mathcal{V}$ and $\overline{\mathcal{V}}$ denote the closure of V in $\mathbb{A}^m_{\mathbb{Z}}$ and in $\mathbb{P}^m_{\mathbb{Z}}$, respectively. Then $\mathcal{V}$ is the affine scheme corresponding to the ideal

$$I(\mathcal{V}) = I(V) \cap \mathbb{Z}[\boldsymbol{X}]$$

and $\overline{\mathcal{V}}$ is the projective scheme corresponding to

$$I(\overline{\mathcal{V}}) = I(\mathcal{V})^{\mathrm{h}} \subseteq \mathbb{Z}[\boldsymbol{Z}],$$

the homogenisation of the ideal $I(\mathcal{V})$.

Consider the projection $\pi\colon \mathbb{P}^m_{\mathbb{Z}} \to \mathrm{Spec}(\mathbb{Z})$ and set

$$\overline{\mathcal{V}}_p = \pi^{-1}(p) \cap \overline{\mathcal{V}}$$

for the fibre over the prime p of the restriction to $\overline{\mathcal{V}}$ of this map. It is a subscheme of the projective space $\mathbb{P}^m_{\mathbb{F}_p}$.

The morphism of schemes $\mathcal{V} \to \mathrm{Spec}(\mathbb{Z})$ is *flat* if there is a family of flat $\mathbb{Z}$-algebras $\mathcal{A}_j$, $j \in J$, such that their associated affine schemes form an open covering of $\mathcal{V}$, namely $\mathcal{V} = \bigcup_{j\in J} \mathrm{Spec}(\mathcal{A}_j)$. Since $\mathbb{Z}$ is a principal ideal domain, the $\mathbb{Z}$-algebras $\mathcal{A}_j$, $j \in J$, are flat if and only if they are torsion free [Liu02, Corollary 1.2.5]. The flatness of an algebra over a ring is a property concerning extensions of scalars. At the geometric level, this property ensures a certain continuity behavior of the fibres of the morphism, see [Liu02, §4.3] for more details.

Lemma 2.4. *Let notation be as above.*

(1) *The projective scheme $\overline{\mathcal{V}}$ is flat over* $\mathrm{Spec}(\mathbb{Z})$ *and moreover, it is reduced, has pure relative dimension 0, and none of its irreducible components is contained in the hyperplane at infinity.*
(2) *For all $p \in \mathrm{Spec}(\mathbb{Z})$, we have that $\overline{\mathcal{V}}_p$ is a 0-dimensional subscheme of $\mathbb{P}^m_{\mathbb{F}_p}$ of degree T.*
(3) *The inclusion $\overline{\mathcal{V}}_p(\overline{\mathbb{F}}_p) \cap \overline{\mathbb{F}}_p^m \subseteq V_p(\overline{\mathbb{F}}_p)$ holds.*

Proof. For the statement (1), consider the decomposition $V = \bigcup_C C$ into irreducible components. For each C, denote by $\overline{\mathcal{C}}$ its closure in $\mathbb{P}^m_{\mathbb{Z}}$. Then

$$I(\overline{\mathcal{C}}) = (I(C) \cap \mathbb{Z}[\boldsymbol{X}])^{\mathrm{h}} \subseteq \mathbb{Z}[\boldsymbol{Z}],$$

where, as before, J^{h} denotes the homogenisation of the ideal J.

One can verify that this ideal is prime and that $I(\overline{\mathcal{C}}) \cap \mathbb{Z} = \{0\}$. We have that

$$\overline{\mathcal{V}} = \bigcup_C \overline{\mathcal{C}},$$

and so $\overline{\mathcal{V}}$ is a reduced scheme that, by [Liu02, Proposition 4.3.9], is flat over $\mathrm{Spec}(\mathbb{Z})$. Moreover, the Krull dimension of the quotient ring $\mathbb{Z}[\boldsymbol{Z}]/I(\overline{\mathcal{C}})$ is one and $Z_0 \notin I(\overline{\mathcal{C}})$, which respectively implies that $\overline{\mathcal{V}}$ is of pure relative dimension 0 and that none of its irreducible components is contained in the hyperplane at infinity of $\mathbb{P}^m_{\mathbb{Z}}$, as stated.

Now we turn to the statement (2). By the invariance of the Euler-Poincaré characteristic of the fibres of a projective flat morphism, see [Liu02, Proposition 5.3.28], and the fact that the map $\overline{\mathcal{V}} \to \mathrm{Spec}(\mathbb{Z})$ is flat, the Hilbert polynomial of $\overline{\mathcal{V}}_p$ coincides with that of the generic fibre of that map. This generic fibre coincides with the closure of V in $\mathbb{P}^m_{\mathbb{Q}}$, which is a 0-dimensional variety of degree T. It follows that its Hilbert polynomial is the constant T, and so $\overline{\mathcal{V}}_p$ is also a 0-dimensional scheme of degree T.

To prove the statement (3), note first that $\overline{\mathcal{V}}_p(\overline{\mathbb{F}}_p)$ is given by the zero set in $\mathbb{P}^m_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ of the ideal

$$\Big(\sqrt{(F_1, \dots, F_s)} \cap \mathbb{Z}[\boldsymbol{X}]\Big)^{\mathrm{h}} \pmod p \quad \subseteq \mathbb{F}_p[\boldsymbol{Z}].$$

Hence, the intersection $\overline{\mathcal{V}}_p(\overline{\mathbb{F}}_p) \cap \overline{\mathbb{F}}_p^m$ coincides with the zero set in $\overline{\mathbb{F}}_p^m$ of the affinisation of this ideal, obtained by setting $Z_0 \to 1$ and $Z_i \to X_i$, $i = 1, \dots, m$. Denote by I_1 this ideal of $\mathbb{F}_p[\boldsymbol{X}]$.

On the other hand, V_p is given by the zero set in $\overline{\mathbb{F}}_p^m$ of the ideal

$$I_2 = \sqrt{(F_{1,p}, \dots, F_{s,p})} \subseteq \mathbb{F}_p[\boldsymbol{X}]$$

with $F_{1,p}, \dots, F_{s,p}$ as in (2.3). Then (3) follows from the inclusion of ideals $I_1 \supset I_2$. □

2.4. **Eliminants and heights.** We recall the notion of eliminant of a homogeneous ideal as presented by Philippon in [Phi86]. Let R be a principal ideal domain, with group of units $R^\times$ and field of fractions K. Let $\boldsymbol{U} = \{U_0, \dots, U_m\}$ be a further group of $m+1$ variables and consider the general linear form in the variables $\boldsymbol{Z}$ given by

$$L = U_0 Z_0 + \dots + U_m Z_m \in \mathbb{Z}[\boldsymbol{U}][\boldsymbol{Z}].$$

Definition 2.5. *Let $I \subseteq R[\boldsymbol{Z}]$ be a homogeneous ideal. The* eliminant ideal *of I is the ideal of $R[\boldsymbol{U}]$ defined as*

$$\mathfrak{E}(I) = \{F \in R[\boldsymbol{U}] \mid \exists k \geq 0 \quad \text{with } Z_j^k F \in I R[\boldsymbol{U}, \boldsymbol{Z}] + (L) \text{ for } j = 0, \dots, m\}.$$

If $\mathfrak{E}(I)$ is principal, then the eliminant *of I, denoted by* $\mathrm{Elim}(I)$, *is defined as any generator of this ideal.*

The eliminant of an ideal of $R[\boldsymbol{Z}]$ is a homogeneous polynomial, uniquely defined up to a factor in $R^\times$.

In the following proposition, we gather the basic properties of eliminants of 0-dimensional ideals following [Nes77, Phi86]. Given a prime ideal P in some ring and a P-primary ideal Q, the *exponent* of Q, denoted by $e(Q)$, is the least integer $e \geq 1$ such that $P^e \subseteq Q$. Notice that Q is prime if and only if $e(Q) = 1$.

Lemma 2.6. *Let $I \subseteq R[\boldsymbol{Z}]$ be an equidimensional homogeneous ideal defining a 0-dimensional subvariety of $\mathbb{P}^m_K$.*

(1) *The eliminant ideal* $\mathfrak{E}(I)$ *is principal and* $\mathrm{Elim}(I)$ *is well-defined.*
(2) *If* I *is prime and* $(Z_0, \dots, Z_m) \not\subset I$*, then* $\mathrm{Elim}(I)$ *is an irreducible polynomial.*
(3) *Let* $I = \bigcap_i Q_i$ *be the minimal primary decomposition of* I *and set* $P_i = \sqrt{Q_i}$*. Then there exists* $\mu \in R^\times$ *such that*

$$\mathrm{Elim}(I) = \mu \prod_i \mathrm{Elim}(P_i)^{e(Q_i)}.$$

(4) *Let* $V(I)(\overline{K})$ *be the zero set of* I *in* $\mathbb{P}^m_K(\overline{K})$*. Then*

$$\mathrm{Elim}(I) = \lambda \prod_{\eta \in V(I)(\overline{K})} L(\eta)^{e_\eta},$$

with $\lambda \in K^\times$ *and where* e_η *denotes the exponent of the primary component associated to the point* η*. In particular,* $I \otimes_R K$ *is radical if and only if* $\mathrm{Elim}(I)$ *is squarefree.*

Proof. These statements are either contained or can be immediately extracted from results in [Nes77, Phi86]. Precisely, the statement (1) is [Nes77, Proposition 2(1)] or [Phi86, Lemma 1.8]. The statement (2) is contained in [Phi86, Proposition 1.3(ii)]. The statement (3) follows from [Nes77, Corollary to Proposition 3]. The last claim (4) follows from (3) and the proof of [Phi86, Lemma 1.8]. □

Lemma 2.7. *Let notation be as in §2.3. In particular,* V *is the* 0*-dimensional subvariety of* $\mathbb{A}^m_{\mathbb{Q}}$ *defined by the system* F_i, $i = 1, \dots, s$, $\overline{\mathcal{V}}$ *its closure in* $\mathbb{P}^m_{\mathbb{Z}}$*, and* T *the number of points in* $V(\overline{\mathbb{Q}})$*. Then* $\mathfrak{E}(I(\overline{\mathcal{V}}))$ *is a principal ideal and the eliminant* $\mathrm{Elim}(I(\overline{\mathcal{V}})) \in \mathbb{Z}[\boldsymbol{U}]$ *is well-defined. Moreover, this eliminant is a primitive polynomial and we have the factorisation*

$$\mathrm{Elim}(I(\overline{\mathcal{V}})) = \lambda \prod_{(\xi_1,\dots,\xi_m) \in V(\overline{\mathbb{Q}})} (U_0 + \xi_1 U_1 + \dots + \xi_m U_m) \tag{2.5}$$

with $\lambda \in \mathbb{Q}^\times$.

Proof. Set $I = I(\overline{\mathcal{V}})$ for short. The subvariety of $\mathbb{P}^m_{\mathbb{Q}}$ defined by this ideal coincides with $\iota(V)$, the image of V under the standard inclusion (2.4). This subvariety is of dimension 0, and it follows from Lemma 2.6(1) that the eliminant ideal of I is principal and that its eliminant polynomial is well-defined.

By Lemma 2.4(1), the subscheme $\overline{\mathcal{V}} \subset \mathbb{P}^m_{\mathbb{Z}}$ is flat and reduced. Hence, $I = \bigcap_i P_i$ where each P_i is a prime ideal of $\mathbb{Z}[\boldsymbol{Z}]$ which defines a 0-dimensional subvariety of $\mathbb{P}^m_{\mathbb{Q}}$ and $P_i \cap \mathbb{Z} = \{0\}$. By Lemma 2.6(2,4) applied to P_i, each eliminant $\mathrm{Elim}(P_i)$ is an nonconstant irreducible polynomial. Together with Lemma 2.6(3), this implies that $\mathrm{Elim}(I)$ is primitive.

The ideal I is radical and no point of V lies in the hyperplane at infinity of $\mathbb{P}^m_{\mathbb{Q}}$. Then the factorisation (2.5) follows immediately from Lemma 2.6(2, 4). $\square$

Set

$$E_V = \mathrm{Elim}(I(\overline{\mathcal{V}})) \tag{2.6}$$

for short. Our next aim is to bound the height of this polynomial in terms of the degree and the height of the F_i's. To this end, we first recall the notion of Weil height of a finite subset of $\overline{\mathbb{Q}}^m$.

Given a number field $\mathbb{K}$, we denote by $M_{\mathbb{K}}$ its set of places. For each $w \in M_{\mathbb{K}}$, we assume the corresponding absolute value of $\mathbb{K}$, denoted by $|\cdot|_w$, extends either the Archimedean or a p-adic absolute value of $\mathbb{Q}$, with their standard normalisation.

Let $\boldsymbol{\eta} \in \mathbb{P}^m_{\mathbb{Q}}(\overline{\mathbb{Q}})$ and choose a number field $\mathbb{K}$ such that $\boldsymbol{\eta} = (\eta_0 : \dots : \eta_m)$ with $\eta_i \in \mathbb{K}$. The *Weil height* of $\boldsymbol{\eta}$ is defined as

$$\widehat{\mathrm{h}}(\boldsymbol{\eta}) = \sum_{w \in M_{\mathbb{K}}} \frac{[\mathbb{K}_w : \mathbb{Q}_w]}{[\mathbb{K} : \mathbb{Q}]} \log \max\{|\eta_0|_w, \dots, |\eta_m|_w\},$$

where $\mathbb{K}_w$ and $\mathbb{Q}_w$ denote the w-adic completion of $\mathbb{K}$ and $\mathbb{Q}$, respectively. This formula does not depend neither on the choice of homogeneous coordinates of $\boldsymbol{\eta}$ nor on the number field $\mathbb{K}$. Hence, it defines a function

$$\widehat{\mathrm{h}} \colon \mathbb{P}^m_{\mathbb{Q}}(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}.$$

For a point of $\overline{\mathbb{Q}}^m$, we define its Weil height as the Weil height of its image in $\mathbb{P}^m_{\mathbb{Q}}(\overline{\mathbb{Q}})$ *via* the inclusion (2.4) and, for a finite subset of $\overline{\mathbb{Q}}^m$, we define its Weil height as the sum of the Weil height of its points.

Since the F_i's have integer coefficients, the points of V lie in $\overline{\mathbb{Q}}^m$. If we write

$$V(\mathbb{C}) = Z(F_1, \dots, F_s) = \{\boldsymbol{\xi}_1, \dots, \boldsymbol{\xi}_T\}$$

with $\boldsymbol{\xi}_j \in \overline{\mathbb{Q}}^m$, then the Weil height of this set is given by

$$\begin{aligned} \widehat{\mathrm{h}}(V) &= \sum_{i=1}^{T} \widehat{\mathrm{h}}(\boldsymbol{\xi}_i) \\ &= \sum_{j=1}^{T} \sum_{w \in M_{\mathbb{K}}} \frac{[\mathbb{K}_w : \mathbb{Q}_w]}{[\mathbb{K} : \mathbb{Q}]} \log \max\{1, |\xi_{j,1}|_w, \dots, |\xi_{j,m}|_w\}. \end{aligned} \tag{2.7}$$

We refer to [BG06] for a more detailed background on heights.

The notion of Weil height of points extends to projective varieties. This extension is usually called the "normalised" or "canonical" height and also denoted by the operator $\widehat{\mathrm{h}}$, see for instance [PS08, §I.2] or [DKS13, §2.3]. For an affine variety $Z \subset \mathbb{A}^m_{\mathbb{Q}}$, we respectively denote by $\deg Z$ and $\widehat{\mathrm{h}}(Z)$ the sum of the degrees and of the canonical heights of the Zariski closure in $\mathbb{P}^m_{\mathbb{Q}}$ of its irreducible components. We also define the dimension of Z, denoted by $\dim Z$, as the maximum of the dimensions of its irreducible components.

The following is a version of the arithmetic Bézout inequality.

Lemma 2.8. *Let $Z \subset \mathbb{A}^m_{\mathbb{Q}}$ be a variety and $G_i \in \mathbb{Z}[\boldsymbol{X}]$, $i = 1, \dots, t$. Set*

$$d_i = \deg G_i, \qquad h = \max_{i=1,\dots,t} \mathrm{h}(G_i), \qquad m_0 = \min\{\dim Z, m\},$$

and assume that $d_1 \geq \dots \geq d_t$. Then

$$\widehat{\mathrm{h}}(Z \cap V(G_1, \dots, G_t)) \leq \prod_{i=1}^{m_0} d_i \bigg(\widehat{\mathrm{h}}(Z) + \bigg(\sum_{i=1}^{m_0} \frac{1}{d_i}\bigg) h \deg Z \\ + m_0 \log(m+1) \deg Z\bigg).$$

Proof. Let $C \subseteq \mathbb{A}^m_{\mathbb{Q}}$ be an irreducible subvariety and $F \in \mathbb{Z}[\boldsymbol{X}]$ a polynomial such that the hypersurface $V(F) \subseteq \mathbb{A}^m_{\mathbb{Q}}$ intersects C properly. From [DKS13, Theorem 2.58], we deduce that

$$\widehat{\mathrm{h}}(C \cap V(F)) \leq \widehat{\mathrm{h}}(C) \deg F + (\mathrm{h}(F) + \deg F \log(m+1)) \deg C. \tag{2.8}$$

The stated bound now follows by repeating the scheme of the proof of [KPS01, Corollary 2.11] for the canonical height instead of the Fubini-Study one, and using (2.8) instead of the inequality in the second line of [KPS01, Page 555]. □

Let $F_1, \dots, F_s \in \mathbb{Z}[\boldsymbol{X}]$ and let $V \subseteq \mathbb{A}^m_{\mathbb{Q}}$ be the 0-dimensional subvariety defined by this system of polynomials, as in §2.3. Also set

$$d = \max_{i=1,\dots,s} \deg F_i \qquad \text{and} \qquad h = \max_{i=1,\dots,s} \mathrm{h}(F_i).$$

Corollary 2.9. *Write $V(\mathbb{C}) = \{\boldsymbol{\xi}_1, \dots, \boldsymbol{\xi}_T\}$ with $\boldsymbol{\xi}_j \in \overline{\mathbb{Q}}^m$. Then*

$$T \leq d^m \qquad \textit{and} \qquad \sum_{i=1}^{T} \widehat{\mathrm{h}}(\boldsymbol{\xi}_i) \leq m d^{m-1}(h + d \log(m+1)).$$

Proof. The first inequality is given by the Bézout theorem. For the rest, we have that $\deg \mathbb{A}^m_{\mathbb{Q}} = 1$ and, by [DKS13, Proposition 2.39(4)], $\widehat{\mathrm{h}}(\mathbb{A}^m_{\mathbb{Q}}) = 0$. The statement then follows from Lemma 2.8 and the inequalities $0 \leq m$ and $d_i \leq d$. □

Lemma 2.10. *With notation as above, let E_V denote the eliminant of the ideal $I(\overline{\mathcal{V}})$ as in (2.6). Then*

$$\deg_{U_0} E_V = \deg E_V = T \leq d^m$$

and

$$\mathrm{h}(E_V) \leq m d^{m-1} h + (m+1) d^m \log(m+1).$$

Proof. Set

$$Q = \prod_{j=1}^{T} (U_0 + \xi_{j,1} U_1 + \ldots + \xi_{j,m} U_m) \in \mathbb{Q}[\boldsymbol{U}]$$

so that, by the factorisation (2.5) of Lemma 2.7 we have $E_V = \lambda Q$ with $\lambda \in \mathbb{Q}^\times$. The formula for the degrees of the eliminant follows readily from this.

For a polynomial F over $\mathbb{Q}$, we denote by $\|F\|_{\infty,1}$ the ℓ^1-norm of its vector of coefficients with respect to the Archimedean absolute value of $\mathbb{Q}$. Then

$$\mathrm{h}(E_V) \leq \log \|E_V\|_{\infty,1} = \log \|Q\|_{\infty,1} + \log |\lambda|_\infty. \tag{2.9}$$

Since E_V is primitive, for $v \in M_{\mathbb{Q}} \setminus \{\infty\}$,

$$0 = \log \|E_V\|_v = \log \|Q\|_v + \log |\lambda|_v,$$

where $\|Q\|_v$ is defined as the maximum norm of the vector of the coefficients of Q with respect to the absolute value $|\cdot|_v$. Summing up over all places and using the product formula, we obtain

$$\log \|E_V\|_{\infty,1} = \log \|Q\|_{\infty,1} + \sum_{v \in M_{\mathbb{Q}} \setminus \{\infty\}} \log \|Q\|_v. \tag{2.10}$$

Let $\mathbb{K}$ be a number field of definition of $\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_T$, and denote by $M_{\mathbb{K}}^\infty$ and $M_{\mathbb{K}}^0$ the set of Archimedean and non-Archimedean places of $\mathbb{K}$, respectively. For each $w \in M_{\mathbb{K}}^\infty$ and a polynomial F over $\mathbb{K}$, we denote by $\|F\|_{w,1}$ the ℓ^1-norm of its vector of coefficients with respect to the absolute value $|\cdot|_w$. Then, by the compatibility between places and finite extensions,

$$\begin{aligned} &\log \|Q\|_{\infty,1} + \sum_{v \in M_{\mathbb{Q}} \setminus \{\infty\}} \log \|Q\|_v \\ &\quad = \sum_{w \in M_{\mathbb{K}}^\infty} \frac{[\mathbb{K}_w : \mathbb{Q}_w]}{[\mathbb{K} : \mathbb{Q}]} \log \|Q\|_{w,1} + \sum_{w \in M_{\mathbb{K}}^0} \frac{[\mathbb{K}_w : \mathbb{Q}_w]}{[\mathbb{K} : \mathbb{Q}]} \log \|Q\|_w. \end{aligned} \tag{2.11}$$

For $w \in M_K^\infty$, by the sub-additivity of $\log \|\cdot\|_{w,1}$,

$$\begin{aligned} \log \|Q\|_{w,1} &\leq \sum_{j=1}^{T} \log \|U_0 + \xi_{j,1} U_1 + \ldots + \xi_{j,m} U_m\|_{w,1} \\ &\leq \sum_{j=1}^{T} \log \max\{1, |\xi_{j,1}|_w, \ldots, |\xi_{j,m}|_w\} + T \log(m+1). \end{aligned} \tag{2.12}$$

On the other hand, for $w \in M_{\mathbb{K}}^0$,

$$\begin{aligned} \log\|Q\|_w &= \sum_{j=1}^{T} \log\|U_0 + \xi_{j,1}U_1 + \ldots + \xi_{j,m}U_m\|_w \\ &= \sum_{j=1}^{T} \log\max\{1, |\xi_{j,1}|_w, \ldots, |\xi_{j,m}|_w\}. \end{aligned} \tag{2.13}$$

If follows from (2.9), (2.10), (2.11), (2.12), (2.13) and (2.7) that

$$\mathrm{h}(E_V) \leq \sum_{i=1}^{T} \widehat{\mathrm{h}}(\boldsymbol{\xi}_i) + T\log(m+1).$$

The statement then follows from the bound for the Weil height in Corollary 2.9. □

Set

$$L^{\mathrm{aff}} = U_0 + U_1X_1 + \ldots + U_nX_n \in \mathbb{Z}[\boldsymbol{U}, \boldsymbol{X}].$$

By construction, E_V vanishes on the zero locus of $F_1, \ldots, F_s$ and L^{aff} in $\mathbb{C}^{m+1} \times \mathbb{C}^m$. By Hilbert's Nullstellensatz, there exist $\alpha, N \in \mathbb{N}$ such that

$$\alpha E_V^N \in (F_1, \ldots, F_s, L^{\mathrm{aff}}) \subseteq \mathbb{Z}[\boldsymbol{U}, \boldsymbol{X}].$$

We use the effective version of this result [DKS13, Theorem 2] to bound the integer α.

Lemma 2.11. *With notation as above, there exist $\alpha, N \in \mathbb{N}$ such that*

$$\alpha E_V^N \in (F_1, \ldots, F_s, L^{\mathrm{aff}}) \subseteq \mathbb{Z}[\boldsymbol{U}, \boldsymbol{X}]$$

and

$$\log\alpha \leq A_1(m)d^{m+\min\{s,2m+1\}}h + A_2(m,s)d^{m+\min\{s,2m+2\}}$$

with

$$\begin{aligned} A_1(m) &= 10m + 4, \\ A_2(m,s) &= (54m + 98)\log(2m+5) + 24(m+1)\log\max\{1, s - 2m\}. \end{aligned}$$

Proof. The system of polynomials $F_1, \ldots, F_s, L^{\mathrm{aff}}$ verifies the bounds

$$\deg F_j \leq d, \quad \deg L^{\mathrm{aff}} = 2, \quad \mathrm{h}(F_j) \leq h, \quad \mathrm{h}(L^{\mathrm{aff}}) = 0.$$

The case when $d = 1$ can be easily treated applying Cramer's rule to the system of linear equations $F_i = 0$, $i = 1, \ldots, s$. Hence, we assume that $d \geq 2$.

We apply [DKS13, Theorem 2] to the variety $\mathbb{A}_{\mathbb{Q}}^{2m+1}$ and the polynomials E_V, $F_1, \ldots, F_s$ and L^{aff}. From the statement of [DKS13, Theorem 2], we consider the parameter D and the sum over ℓ in the bound on α, which we denote by Σ. In our situation, the parameters n and r in the notation of this theorem, are equal to $2m + 1$.

For $s+1 \leq 2m+2$, we have that $D \leq 2d^s$ and $D\Sigma \leq 2sd^{s-1}h + d^s h \leq (s+1)d^s h$ whereas, for $s+1 > 2m+2$, we have that $D \leq d^{2m+2}$ and $D\Sigma \leq (2m+2)hd^{2m+1}$. In either case,

$$D \leq 2d^{\min\{s,2m+2\}} \qquad \text{and} \qquad D\Sigma \leq (2m+2)d^{\min\{s,2m+1\}}h.$$

Thus, since $\deg \mathbb{A}_{\mathbb{Q}}^{2m+1} = 1$ and $\widehat{\mathrm{h}}(\mathbb{A}_{\mathbb{Q}}^{2m+1}) = 0$, it follows that

$$\begin{aligned}\log \alpha \leq 2D \deg E_V \Big(& \frac{3\mathrm{h}(E_V)}{2\deg E_V} + \Sigma \\ & + ((12m+6)+17)\log((2m+1)+4) \\ & + 3(2m+2)\log(\max\{1, s-2m\})\Big) \\ \leq\; & 6d^{\min\{s,2m+2\}}\mathrm{h}(E_V) + 2(2m+2)d^{\min\{s,2m+1\}}h \deg E_V \\ & + 4d^{\min\{s,2m+2\}} \deg E_V \big((12m+23)\log(2m+5) \\ & + 6(m+1)\log\max\{1, s-2m\}\big).\end{aligned}$$

Applying Lemma 2.10, we obtain

$$\begin{aligned}\log \alpha \leq\; & 6d^{\min\{s,2m+2\}} \left(md^{m-1}h + (m+1)d^m \log(m+1)\right) \\ & + 2(2m+2)d^{m+\min\{s,2m+1\}}h \\ & + 4d^{m+\min\{s,2m+2\}}\big((12m+23)\log(2m+5) \\ & + 6(m+1)\log\max\{1, s-2m\}\big).\end{aligned}$$

The coefficient multiplying h in the expression above can be bounded by

$$\begin{aligned} & 6d^{m+\min\{s,2m+2\}-1}m + 2d^{m+\min\{s,2m+1\}}(2m+2) \\ & \leq 6d^{m+\min\{s,2m+1\}}m + 2d^{m+\min\{s,2m+1\}}(2m+2) \\ & = A_1(m,s)d^{m+\min\{s,2m+1\}}.\end{aligned}$$

By replacing $\log(m+1)$ with $\log(2m+5)$ and after simple calculations, we obtain the desired expression for $A_2(m,s)$. □

We now recall the standard bound for the height of the composition of polynomials with integer coefficients, see, for instance, [KPS01, Lemma 1.2(1.c)].

Lemma 2.12. *Let $F \in \mathbb{Z}[Y_1, \dots, Y_\ell]$ and $G_1, \dots, G_\ell \in \mathbb{Z}[\boldsymbol{X}]$. Set*

$$d = \max_{i=1,\dots,\ell} \deg G_i \qquad \text{and} \qquad h = \max_{i=1,\dots,\ell} \mathrm{h}(G_i).$$

Then

$$\mathrm{h}\left(F(G_1, \dots, G_\ell)\right) \leq \mathrm{h}(F) + \deg F\left(h + \log(\ell+1) + d\log(m+1)\right).$$

Lemma 2.13. *Let notation be as above. Then there exists $\beta \in \mathbb{N}$ such that*

$$\log \beta \leq B_1(m)d^{2m-1}h + B_2(m)d^{2m}$$

with

$$B_1(m) = 2m \qquad \textit{and} \qquad B_2(m) = (2m+4)\log(m+1) + 4m + 2,$$

such that, if p is a prime number not dividing β, then the reduction of E_V modulo p is a squarefree polynomial of degree T in the variable U_0.

Proof. By Lemma 2.10, $\deg_{U_0} E_V = T$. Let β_0 be the coefficient of the monomial U_0^T in E_V. If $p \nmid \beta_0$, then reduction of E_V modulo p has also degree T in the variable U_0.

In addition, E_V is squarefree and so

$$\Delta := \mathrm{Res}_{U_0}\left(E_V, \frac{\partial E_V}{\partial U_0}\right) \in \mathbb{Z}[U_1, \dots, U_m]$$

is a nonzero polynomial. If p does not divide one of the nonzero coefficients of this polynomial, then $E_V \pmod{p}$ is also squarefree. Thus we choose β as the absolute value of β_0 times any nonzero coefficient of Δ.

The logarithm of $|\beta_0|$ is bounded by the height of E_V. Hence, by Lemma 2.10,

$$\log|\beta_0| \le md^{m-1}h + (m+1)d^m \log(m+1). \tag{2.14}$$

By [Som04, Theorem 1.1], the Sylvester resultant of two generic univariate polynomials of respective degrees T and $T-1$, has $2T+1$ coefficients, degree $2T-1 \le 2d^m - 1$ and height bounded by $2T\log T \le 2md^m \log d$. By Lemma 2.10,

$$\deg E_V, \deg \frac{\partial E_V}{\partial U_0} \le d^m,$$
$$\mathrm{h}(E_V), \mathrm{h}\left(\frac{\partial E_V}{\partial U_0}\right) \le md^{m-1}h + (m+1)d^m\log(m+1) + m\log d.$$

Hence, specializing this generic resultant in the coefficients of E_V and $\partial E_V/\partial U_0$, seen as polynomial in the variable U_0, and using Lemma 2.12 with $F = \Delta$, $\ell = 2T+1 \le 2d^m + 1$ and $k = m$, we get

$$\begin{aligned}
\mathrm{h}(\Delta) \le{}& 2md^m \log d \\
&+ (2d^m - 1)\big(md^{m-1}h + (m+1)d^m \log(m+1) + m\log d \\
&+ \log(2d^m+2) + d^m\log(m+1)\big) \\
\le{}& 2md^m\log d \\
&+ (2d^m-1)\big(md^{m-1}h + (m+2)d^m\log(m+1) + m\log d \\
&+ \log(2d^m+2)\big).
\end{aligned}$$

Taking into account that $\log(2d^m+2) \le (m+1)d$, we get

$$\begin{aligned}
\mathrm{h}(\Delta) \le (2d^m - 1)\left(md^{m-1}h + (m+2)d^m\log(m+1)\right)& \\
+ 2d^m(2m+1).&
\end{aligned} \tag{2.15}$$

Adding (2.14) and (2.15), we easily derive the stated result. □

2.5. **Proof of Theorem 2.1.** We assume that $d \geq 2$ as otherwise the result is trivial by the Hadamard bound on the determinant of the corresponding system of linear equations.

Set $\mathfrak{A} = \alpha\beta$ with α as in Lemma 2.11 and β as in Lemma 2.13. If $p \nmid \mathfrak{A}$, then $p \nmid \beta$ and, by Lemma 2.13, the reduction of the eliminant E_V modulo p is a squarefree polynomial of degree T in the variable U_0.

Recall that $\overline{\mathcal{V}}_p$ denotes the fibre of the scheme $\overline{\mathcal{V}}$ over the prime p. This is a subscheme of $\mathbb{P}^m_{\mathbb{F}_p}$. From the definition of the eliminant ideal, we can see that $\mathrm{Elim}(I(\overline{\mathcal{V}}_p))$ divides $E_V \pmod p$. Since this latter polynomial is squarefree, it follows that $\mathrm{Elim}(I(\overline{\mathcal{V}}_p))$ is squarefree too.

By Lemma 2.6(4), this implies that the subcheme $\overline{\mathcal{V}}_p$ is reduced and, by Lemma 2.4(2), it is of degree T. Applying Lemma 2.6(4) again, we deduce that $\mathrm{Elim}(I(\overline{\mathcal{V}}_p))$ has degree T and so

$$\mathrm{Elim}(I(\overline{\mathcal{V}}_p)) \equiv \lambda E_V \pmod p$$

with $\lambda \in \mathbb{F}_p^\times$. By Lemma 2.13, the polynomial $E_V \pmod p$ has degree T in the variable U_0. This implies that the subscheme $\overline{\mathcal{V}}_p$ is contained in the open subset $\mathbb{A}^m_{\mathbb{F}_p}$. Hence, $\overline{\mathcal{V}}_p$ is a subvariety of degree T which is contained in V_p.

If p is a prime not dividing $\mathfrak{A}$, then $p \nmid \alpha$ and so α is invertible modulo p. Write $L_p^{\mathrm{aff}} \in \mathbb{F}_p[\boldsymbol{U}, \boldsymbol{X}]$ for the reduction modulo p of L^{aff}. Then

$$E_V^N \pmod p \in (F_{1,p}, \dots, F_{s,p}, L_p^{\mathrm{aff}}) \subseteq \mathbb{F}_p[\boldsymbol{U}, \boldsymbol{X}]$$

with $F_{1,p}, \dots, F_{s,p}$ as in (2.3). Write

$$E_V^N \pmod p = A L_p^{\mathrm{aff}} + \sum_{j=1}^{s} B_j F_{j,p} \tag{2.16}$$

with $A, B_j \in \mathbb{F}_p[\boldsymbol{U}, \boldsymbol{X}]$. Let $\boldsymbol{\xi}$ be a zero of $F_{j,p}$, $j = 1, \dots, s$, in $\overline{\mathbb{F}}_p^m$. Evaluating the equality (2.16) at this point, we obtain

$$E_V^N(\boldsymbol{U}) \pmod p = A(\boldsymbol{U}, \boldsymbol{\xi}) L^{\mathrm{aff}}(\boldsymbol{U}, \boldsymbol{\xi}).$$

It follows that $L_p^{\mathrm{aff}}(\boldsymbol{U}, \boldsymbol{\xi})$ divides $E_V(\boldsymbol{U}) \pmod p$ for every such point. Since for every pair of distinct points $\boldsymbol{\xi}_1$ and $\boldsymbol{\xi}_2$ in $\overline{\mathbb{F}}_p^m$, the linear forms $L_p^{\mathrm{aff}}(\boldsymbol{U}, \boldsymbol{\xi}_1)$ and $L_p^{\mathrm{aff}}(\boldsymbol{U}, \boldsymbol{\xi}_2)$ are coprime, we conclude that the zero set of $F_1, \dots, F_s$ in $\overline{\mathbb{F}}_p^m$ has at most $\deg E_V = T$ points. Hence V_p is of dimension 0 and degree T, as stated.

The bound for $\mathfrak{A}$ follows from the bounds for α in Lemma 2.11 and for β in Lemma 2.13. Indeed, with the notation therein, the quantity $A_1(m) d^{m+\min\{s,2m+1\}} + B_1(m) d^{2m-1}$ can be bounded by

$$(10m+4) d^{m+\min\{s,2m+1\}} + 2m d^{2m-1} \leq (11m+4) d^{3m+1} = C_1(m) d^{3m+1},$$

and $A_2(m,s)d^{m+\min\{s,2m+2\}} + B_2(m)d^{2m-1}$ can be bounded by

$$\begin{aligned}
&\big((54m+98)\log(2m+5)\\
&\qquad + 24(m+1)\log\max\{1,s-2m\}\big)d^{m+\min\{s,2m+2\}}\\
&\qquad\qquad + ((2m+4)\log(m+1)+(4m+2))\,d^{2m}\\
&\qquad \le \big((54m+98)\log(2m+5)+24(m+1)\log\max\{1,s-2m\}\\
&\qquad\qquad + \frac{1}{8}\left((2m+4)\log(m+1)+(4m+2)\right)\big)d^{3m+2}\\
&\qquad \le (55m+99)\log((2m+5)s)d^{3m+2} = d^{3m+2}C_2(m,s)
\end{aligned}$$

with $C_1(m) = 11m+4$ and $C_2(m,s) = (55m+99)\log((2m+5)s)$. Hence

$$\log\mathfrak{A} \le C_1(m)d^{3m+1}h + C_2(m,s)d^{3m+2},$$

concluding the proof.

3. Bounds for the Degrees and the Heights of Products and Compositions of Rational Functions

In this section, we collect several useful bounds on the height of various polynomials and rational functions. These lemmas are used in the proof of our results in §4, §5 and §6, and some of them can be of independent interest.

The following bound on the height of a product of polynomials, which follows from [KPS01, Lemma 1.2], underlines our estimates.

Lemma 3.1. *Let $F_1,\dots,F_s \in \mathbb{Z}[\boldsymbol{X}]$. Then*

$$\begin{aligned}
-2\sum_{i=1}^{s}\deg F_i\log(m+1) \le \mathrm{h}\left(\prod_{i=1}^{s}F_i\right) - \sum_{i=1}^{s}\mathrm{h}(F_i)&\\
\le \sum_{i=1}^{s}\deg F_i\log(m+1).&
\end{aligned}$$

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

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

We already used the bound for the composition of polynomials (see Lemma 2.12). We now specialize it to polynomials with equal number of variables.

Lemma 3.2. *Let $F, G_1,\dots,G_m \in \mathbb{Z}[\boldsymbol{X}]$. Set $d = \max_{i=1,\dots,s}\deg G_i$ and $h = \max_{i=1,\dots,s}\mathrm{h}(G_i)$. Then*

$$\begin{aligned}
&\deg F(G_1,\dots,G_m) \le d\deg F,\\
&\mathrm{h}\left(F(G_1,\dots,G_m)\right) \le \mathrm{h}(F) + h\deg F + (d+1)\deg F\log(m+1).
\end{aligned}$$

The following is and extension of Lemma 3.2 to the composition of rational functions.

Lemma 3.3. *Let $R, S_1, \dots, S_m \in \mathbb{Q}(\boldsymbol{X})$ such that the composition $R(S_1, \dots, S_m)$ is well defined. Set $d = \max_{i=1,\dots,s} \deg S_i$ and $h = \max_{i=1,\dots,s} \mathrm{h}(S_i)$. Then*

$$\deg R(S_1, \dots, S_m) \le dm \deg R,$$
$$\mathrm{h}\left(R(S_1, \dots, S_m)\right) \le \mathrm{h}(R) + h \deg R + (3dm + 1) \deg R \log(m + 1).$$

Proof. Let $R = P/Q$ with coprime $P, Q \in \mathbb{Z}[\boldsymbol{X}]$ and write

$$P = \sum_{\boldsymbol{a}} \alpha_{\boldsymbol{a}} \boldsymbol{X}^{\boldsymbol{a}} \qquad \text{and} \qquad Q = \sum_{\boldsymbol{a}} \beta_{\boldsymbol{a}} \boldsymbol{X}^{\boldsymbol{a}}$$

with $\alpha_{\boldsymbol{a}}, \beta_{\boldsymbol{b}} \in \mathbb{Z}$. We suppose for simplicity that

$$D = \deg P \ge \deg Q,$$

since the other case can be reduced to this one by considering the inverse R^{-1}.

Let also $S_i = F_i/G_i$ with coprime $F_i, G_i \in \mathbb{Z}[\boldsymbol{X}]$. Consider the polynomials

$$B = \prod_j G_j \qquad \text{and} \qquad A_i = F_i \prod_{j \ne i} G_j$$

and set $\boldsymbol{A} = (A_1, \dots, A_m)$. Then $R(S_1, \dots, S_m) = U/V$ with

$$U = \sum_{\boldsymbol{a}} \alpha_{\boldsymbol{a}} B^{D-|\boldsymbol{a}|} \boldsymbol{A}^{\boldsymbol{a}} \qquad \text{and} \qquad V = \sum_{\boldsymbol{a}} \beta_{\boldsymbol{a}} B^{D-|\boldsymbol{a}|} \boldsymbol{A}^{\boldsymbol{a}}.$$

By Lemma 3.1, for each $\boldsymbol{a}$ with $|\boldsymbol{a}| \le D$,

$$\deg(B^{D-|\boldsymbol{a}|} \boldsymbol{A}^{\boldsymbol{a}}) \le mDd, \quad \mathrm{h}(B^{D-|\boldsymbol{a}|} \boldsymbol{A}^{\boldsymbol{a}}) \le mDh + mDd \log(m + 1).$$

Hence $\deg U, \deg V \le mDd$, which gives the degree bound for the rational function $R(S_1, \dots, S_m)$. For the height bound, we have that

$$\begin{aligned} \mathrm{h}(U) &\le h(P) + mDh + mDd \log(m + 1) + \log \binom{D + m}{m} \\ &\le h(R) + mDh + mDd \log(m + 1) + D \log(m + 1), \end{aligned} \tag{3.2}$$

and similarly for V.

Let $\widetilde{U}, \widetilde{V} \in \mathbb{Z}[\boldsymbol{X}]$ coprime with $\widetilde{U}/\widetilde{V} = U/V$. Then $\widetilde{U} \mid U$ and $\widetilde{V} \mid V$. Then, by Lemma 3.1,

$$\mathrm{h}(\widetilde{U}) \le \mathrm{h}(U) + 2 \log(m + 1) \deg U, \tag{3.3}$$

and similarly for $\widetilde{V}$. From (3.2) and (3.3), it follows that

$$\begin{aligned} \mathrm{h}(\widetilde{U}) &\le h(R) + mDh + D(md + 1) \log(m + 1) + 2mDd \log(m + 1) \\ &\le h(R) + mDh + D(3md + 1) \log(m + 1), \end{aligned}$$

and similarly for $\widetilde{V}$, which gives the bound for the height of the composition. $\square$

We now use Lemma 3.2 to bound the degree and height of iterations of polynomial systems.

Lemma 3.4. *Let $F_1, \dots, F_m \in \mathbb{Z}[\boldsymbol{X}]$ be polynomials of degree at most $d \geq 2$ and height at most h. Then, for any positive integer k, the polynomials $F_1^{(k)}, \dots, F_m^{(k)}$ defined by (1.1), are of degree at most d^k and of height at most*

$$h\frac{d^k-1}{d-1} + d(d+1)\frac{d^{k-1}-1}{d-1}\log(m+1).$$

Proof. The bound on the degree is trivial, and the inequality for the height also follows straightforwardly by induction on the number of iterates k. Indeed, for $k=1$ we have equality by definition. Suppose the statement is true for the first $k-1$ iterates. For every $i=1,\dots,m$, we apply Lemma 3.2 to the polynomial

$$F_i^{(k)} = F_i^{(k-1)}(F_1,\dots,F_m)$$

and we get that the height of this polynomial is bounded by

$$\begin{aligned} \mathrm{h}(F_i^{(k-1)}) &+ (h+(d+1)\log(m+1))\deg F_i^{(k-1)} \\ &\leq h\frac{d^{k-1}-1}{d-1} + d(d+1)\frac{d^{k-2}-1}{d-1}\log(m+1) \\ &\qquad + (h+(d+1)\log(m+1))d^{k-1} \\ &\leq h\frac{d^k-1}{d-1} + d(d+1)\frac{d^{k-1}-1}{d-1}\log(m+1), \end{aligned}$$

which concludes the proof. □

For rational functions we apply Lemma 3.3 to derive a similar result.

Lemma 3.5. *Let $R_1,\dots,R_m \in \mathbb{Q}(\boldsymbol{X})$ be rational functions of degree at most d and height at most h. If either $d \geq 2$ or $m \geq 2$ then, for any positive integer k, the rational functions $R_1^{(k)},\dots,R_m^{(k)}$ defined by (1.1), are of degree at most $d^k m^{k-1}$, and of height at most*

$$\left(1 + d\frac{d^{k-1}m^{k-1}-1}{dm-1}\right)h + d(3dm+1)\frac{d^{k-1}m^{k-1}-1}{dm-1}\log(m+1).$$

Proof. The bound for the degree follows easily from Lemma 3.3. We prove the bound for the height by induction on k. For $k=1$ the bound is trivial. For $k \geq 2$, we assume that the bound holds for the first $k-1$ iterates.

Applying Lemma 3.3 with R_i and $R_i^{(k-1)}$, $i = 1, \ldots, m$, and the induction hypothesis, we obtain that $\mathrm{h}(R_i^{(k)})$ is bounded by

$$\begin{aligned}
&\mathrm{h}(R_i^{(k-1)}) + h \deg(R_i^{(k-1)}) + (3dm+1)\deg(R_i^{(k-1)}) \log(m+1)\\
&\qquad \le \left(1 + d\frac{d^{k-2}m^{k-2}-1}{dm-1}\right) h\\
&\qquad\qquad + d(3dm+1)\frac{d^{k-2}m^{k-2}-1}{dm-1}\log(m+1)\\
&\qquad\qquad\qquad + hd^{k-1}m^{k-2} + (3dm+1)d^{k-1}m^{k-2}\log(m+1)\\
&\qquad = \left(1 + d\frac{d^{k-1}m^{k-1}-1}{dm-1}\right) h\\
&\qquad\qquad + d(3dm+1)\frac{d^{k-1}m^{k-1}-1}{dm-1}\log(m+1),
\end{aligned}$$

where we have used the identity

$$d\frac{d^{k-2}m^{k-2}-1}{dm-1} + d^{k-1}m^{k-2} = d\frac{d^{k-1}m^{k-1}-1}{dm-1}.$$

□

4. Periodic Points

4.1. **Definitions and main results.** We start with the following standard definition of k-periodicity.

Definition 4.1. *Let K be a field and $\boldsymbol{R} \in K(\boldsymbol{X})^m$ a system of rational functions as in (2.1). Given $k \ge 1$, we say that $\boldsymbol{w} \in \overline{K}^m$ is* k-periodic *if the element $\boldsymbol{w}_k$ exists in the orbit (2.2) and we have $\boldsymbol{w}_k = \boldsymbol{w}_0$.*

In this definition, we do not request that k is the smallest integer with this property. On the other hand, this notion of k-periodicity is more restrictive than the condition $\boldsymbol{R}^{(k)}(\boldsymbol{w}) = \boldsymbol{w}_0$, see the discussion after (2.2).

We first prove the following result for systems of rational functions.

Theorem 4.2. *Let $m, d \in \mathbb{N}$ with $d, m \ge 2$, and $\boldsymbol{R} = (R_1, \ldots, R_m)$ be a system of m rational functions in $\mathbb{Q}(\boldsymbol{X})$ of degree at most d and of height at most h. Assume that $\boldsymbol{R}$ has finitely many periodic points of order k over $\mathbb{C}$. Then there exists an integer $\mathfrak{A}_k \ge 1$ with*

$$\log \mathfrak{A}_k \ll_{d,h,m} (dm)^{k(3m+5)}$$

such that, if p is a prime number not dividing $\mathfrak{A}_k$, then the reduction of $\boldsymbol{R}$ modulo p has at most $(2m^k d^k)^{m+1}$ periodic points of order k.

In the particular case of polynomials, the bound of Theorem 4.2 simplifies as follows:

Theorem 4.3. *Let $d, m \geq 2$, and $\boldsymbol{F} = (F_1, \ldots, F_m)$ be a system of m polynomials in $\mathbb{Z}[\boldsymbol{X}]$ of degree at most d and of height at most h. Assume that $\boldsymbol{F}$ has finitely many periodic points of order k over $\mathbb{C}$. Then there exists an integer $\mathfrak{A}_k \geq 1$ with*

$$\log \mathfrak{A}_k \ll_{d,h,m} d^{k(3m+2)}$$

such that, if p is a prime number not dividing $\mathfrak{A}_k$, then the reduction of $\boldsymbol{F}$ modulo p has at most d^{km} periodic points of order k.

Using these theorems, it is possible to recover some of the results of Silverman and of Akbary and Ghioca, that give lower bounds on the period length which are roughly of order $\log\log p$ for all primes p [Sil08, Corollary 12], and of order $\log p$ for almost all of them [AG09, Theorem 1.1(1)], see [CDO+18, Corollaries 2.3 and 2.4].

Similarly, Theorems 4.2 and 4.3 can be used with k of order $\log p$ and $\log\log p$ for almost all and all primes p, respectively, to get nontrivial upper bounds on the number of periodic points of order k (or even at most k).

4.2. **Proof of Theorem 4.2.** The result is a direct consequence of Theorem 2.1 and Lemma 3.5. Indeed, let $\boldsymbol{R}^{(k)}$ be the iteration of the system of rational functions $\boldsymbol{R}$ as in (1.1). As in (1.2), write

$$R_i^{(k)} = \frac{F_{i,k}}{G_{i,k}}$$

with coprime $F_{i,k}, G_{i,k} \in \mathbb{Z}[\boldsymbol{X}]$ and $G_{i,k} \neq 0$, and consider then the system of equations

$$F_{i,k} - X_i G_{i,k} = 0, \qquad i = 1, \ldots, m.$$

From the solutions to this system of equations, we have to extract those that come from the poles of $R_i^{(j)}$, $j \leq k$, that is, from the zeroes of $\prod_{i=1}^m \prod_{j=1}^k G_{i,j}$. For this we introduce a new variable X_0, and thus, the set of k-periodic points of $\boldsymbol{R}$ coincides with the zero set

$$V_k = Z\left(F_{1,k} - X_1 G_{1,k}, \ldots, F_{m,k} - X_m G_{m,k}, 1 - X_0 \prod_{i=1}^m \prod_{j=1}^k G_{i,j}\right).$$

By Lemma 3.5 and the fact that $dm \geq 2$:

$$\deg\left(X_0 \prod_{i=1}^m \prod_{j=1}^k G_{i,j}\right) \leq 1 + m \sum_{j=1}^k d^j m^{j-1} \leq 2(dm)^k. \tag{4.1}$$

Further, by Lemmas 3.1 and 3.5,

$$\begin{aligned}
\mathrm{h}\left(X_0\prod_{i=1}^{m}\prod_{j=1}^{k}G_{i,j}\right) &= \mathrm{h}\left(\prod_{i=1}^{m}\prod_{j=1}^{k}G_{i,j}\right)\\
&\le 2(dm)^k \log(m+1) + \sum_{i=1}^{m}\sum_{j=1}^{k}\mathrm{h}\left(G_{i,j}\right)\\
&\le 2(dm)^k \log(m+1) + m\Bigg(\sum_{j=1}^{k}\left(1+d\frac{d^{j-1}m^{j-1}-1}{dm-1}\right)h\\
&\qquad\qquad + d(3dm+1)\frac{d^{j-1}m^{j-1}-1}{dm-1}\log(m+1)\Bigg)\\
&\le 2(dm)^k \log(m+1) + m\Big(4d(dm)^{k-2}h\\
&\qquad\qquad + 2d(3dm+1)(dm)^{k-1}\log(m+1)\Big).
\end{aligned}$$

Hence

$$\mathrm{h}\left(X_0\prod_{i=1}^{m}\prod_{j=1}^{k}G_{i,j}\right) \ll_{d,h,m} (dm)^k.$$

Also, for every $i=1,\ldots,m$, we easily see that Lemma 3.5 and the bound (3.1) yield

$$\deg\left(F_{i,k}-X_iG_{i,k}\right) \le d^k m^{k-1}+1,$$

and

$$\begin{aligned}
\mathrm{h}\left(F_{i,k}-X_iG_{i,k}\right) &\le \mathrm{h}\left(R_i^{(k)}\right)+\log 2\\
&\le \left(1+d\frac{d^{k-1}m^{k-1}-1}{dm-1}\right)h\\
&\qquad + d(3dm+1)\frac{d^{k-1}m^{k-1}-1}{dm-1}\log(m+1)+\log 2.
\end{aligned}$$

Hence

$$\mathrm{h}\left(F_{i,k}-X_iG_{i,k}\right) \ll_{d,h,m} d^k m^{k-1}.$$

We apply now Theorem 2.1 (with $s=m+1$ polynomials and $m+1$ variables) and derive

$$\log\mathfrak{A}_k \ll_{d,h,m} (dm)^{k+k(3(m+1)+1)}h+(dm)^{k(3(m+1)+2)} \ll_{d,h,m} (dm)^{k(3m+5)}.$$

Next, we denote by N_k the number of points of V_k over $\mathbb{C}$, which is equal to the number of periodic points of order k of $R_1,\ldots,R_m$ over $\mathbb{C}$. Using the degree bounds (4.1), by Bézout theorem we obtain

$$N_k \le 2(md)^k\left(m^kd^k+1\right)^m \le (2m^kd^k)^{m+1},$$

which yields the desired bound.

4.3. **Proof of Theorem 4.3.** As in the proof of Theorem 4.2, the result is an immediate consequence of Theorem 2.1 and Lemma 3.4. Indeed, we apply Theorem 2.1 with

$$V_k = Z(F_1^{(k)} - X_1, \ldots, F_m^{(k)} - X_m),$$

getting, after simple calculations, that

$$\log \mathfrak{A}_k \ll_{d,h,m} d^{k+k(3m+1)}h + d^{k(3m+2)} \ll_{d,h,m} d^{k(3m+2)}.$$

We now denote by N_k the number of points of V_k over $\mathbb{C}$, which is equal to the number of periodic points of order k of $F_1, \ldots, F_m$ over $\mathbb{C}$. Using Lemma 3.4 and the fact that $N_k \leq d^{km}$, we obtain immediately the desired bound.

4.4. **Lower bounds on the number of k-periodic points.** The bound on the k-periodic points given by Theorem 4.3 is tight for some particular polynomial systems. Indeed, let $d \geq 0$ and consider the system $\boldsymbol{F} = (F_1, \ldots, F_m)$ with $F_i = X_i^d$. For $k \geq 1$, the k-th iterate is given by $F_i^{(k)} = X_i^{d^k}$, $i = 1, \ldots, m$. A k-periodic point is a solution to the system

$$X_i^{d^k} - X_i = 0, \quad i = 1, \ldots, m. \tag{4.2}$$

This system of equations has a finite number of solution over the complex numbers. Set $\mathfrak{A} = d^k - 1$. If p is a prime not dividing $\mathfrak{A}$, then the system of equations (4.2) has exactly d^{km} solutions in $\overline{\mathbb{F}}_p^m$. Hence, the reduction of $\boldsymbol{F}$ modulo p has exactly d^{km} periodic points of order k.

5. Iterations Generically Escaping a Variety

5.1. **Problem formulation and definitions.** We next study the frequency of the orbit intersections of two rational function systems. In the univariate case, Ghioca, Tucker and Zieve [GTZ08, GTZ12] have proved that, if two univariate nonlinear complex polynomials have an infinite intersection of their orbits, then they have a common iterate. No results of this kind are known for arbitrary rational functions.

The analogue of this result by Ghioca, Tucker and Zieve [GTZ08, GTZ12] cannot hold over finite fields. Instead, 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.

As before, we first obtain results for general systems of rational functions and polynomials, and we then obtain stronger bounds for systems of the form (7.1).

Let K be a field and

$$\boldsymbol{R} = (R_1, \ldots, R_m), \qquad R_1, \ldots, R_m \in K(\boldsymbol{X})$$

a system of m rational functions in m variables over K as in (2.1). For $n \ge 1$, we denote by $\boldsymbol{R}^{(n)}$ the n-th iteration of this system, as long as this iteration is well-defined.

Given an initial point $\boldsymbol{w} \in \overline{K}^m$, we consider the sequence given by

$$\boldsymbol{w}_0 = \boldsymbol{w} \qquad \text{and} \qquad \boldsymbol{w}_n = \boldsymbol{R}(\boldsymbol{w}_{n-1}) \text{ for } n \ge 1,$$

as in (2.2). As discussed after (2.2), this sequence terminates when $\boldsymbol{w}_n$ is a pole of the system $\boldsymbol{R}$. Recall that the orbit of $\boldsymbol{w}$ is the subset $\mathrm{Orb}_{\boldsymbol{R}}(\boldsymbol{w}) = \{\boldsymbol{w}_n \mid n \ge 1\} \subset \overline{K}$. We put

$$T(\boldsymbol{w}) = \#\mathrm{Orb}_{\boldsymbol{R}}(\boldsymbol{w}) \in \mathbb{N} \cup \{\infty\}. \tag{5.1}$$

Now let $K = \mathbb{Q}$ and, for $n \ge 1$, write

$$R_i^{(n)} = \frac{F_{i,n}}{G_{i,n}}$$

with coprime $F_{i,n}, G_{i,n} \in \mathbb{Z}[\boldsymbol{X}]$ and $G_{i,n} \ne 0$, as in (1.2). Given a prime p such that $G_{i,j} \not\equiv 0 \pmod p$, $j = 1, \ldots, n$, we can consider the reduction modulo p of the iteration $\boldsymbol{R}^{(n)}$. We denote it by

$$\boldsymbol{R}_p^{(n)} = \left(R_{1,p}^{(n)}, \ldots, R_{m,p}^{(n)}\right) \in \mathbb{F}_p(\boldsymbol{X})^m.$$

Let $V \subset \mathbb{A}_{\mathbb{Q}}^m$ be the affine algebraic variety over $\mathbb{Q}$ defined by a system of polynomials $P_i \in \mathbb{Z}[\boldsymbol{X}]$, $i = 1, \ldots, s$. For a prime p, we denote by $V_p \subset \mathbb{A}_{\mathbb{F}_p}^m$ the variety over $\mathbb{F}_p$ defined by the reduction modulo p of the system P_i, $i = 1, \ldots, s$.

Let $\boldsymbol{w} \in \overline{\mathbb{F}}_p^m$ be an initial point, $N \in \mathbb{N}$, and suppose that $G_{i,j} \not\equiv 0 \pmod p$, $j = 0, \ldots, N-1$. We then define

$$\mathfrak{V}_{\boldsymbol{w}}(\boldsymbol{R}, V; p, N) = \left\{n \in \{0, \ldots, N-1\} \mid \boldsymbol{R}_p^{(n)}(\boldsymbol{w}) \in V_p(\overline{\mathbb{F}}_p)\right\}.$$

Namely, this is the set of values of $n \in \{0, \ldots, N-1\}$ such that the iterate $\boldsymbol{R}_p^{(n)}(\boldsymbol{w})$ is defined and lies in the set $V_p(\overline{\mathbb{F}}_p)$. One of our goals is obtaining upper bounds on $\#\mathfrak{V}_{\boldsymbol{w}}(\boldsymbol{R}, V; p, N)$ that are uniform in $\boldsymbol{w}$.

We now define the following class of pairs $(\boldsymbol{R}, V)$ of systems of rational functions and varieties:

Definition 5.1. *With notation as above, we say that the iterations of* $\boldsymbol{R}$ generically escape V *if, for every integer $k \ge 1$, the k-th iteration of $\boldsymbol{R}$ is well-defined and the set*

$$\left\{\boldsymbol{w} \in \mathbb{C}^m \mid \left(\boldsymbol{w}, \boldsymbol{R}^{(k)}(\boldsymbol{w})\right) \in V(\mathbb{C}) \times V(\mathbb{C})\right\}$$

is finite.

We expect that this property of generic escape is satisfied for a "random" pair $(\boldsymbol{R}, V)$ consisting of a system and a variety of dimension at most $m/2$.

We consider now two rational function systems $\boldsymbol{R}, \boldsymbol{Q} \in \mathbb{Q}(\boldsymbol{X})^m$. For $N \in \mathbb{N}$, let p be a prime such that that the iterations $\boldsymbol{R}^{(j)}$ and $\boldsymbol{Q}^{(j)}$, $j = 0, \ldots, N-1$, can be reduced modulo p. For $\boldsymbol{u}, \boldsymbol{v} \in \overline{\mathbb{F}}_p^m$, we define

$$\mathfrak{I}_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{R}, \boldsymbol{Q}; p, N) = \left\{ n \in \{0, \ldots, N-1\} \mid \boldsymbol{R}_p^{(n)}(\boldsymbol{u}) = \boldsymbol{Q}_p^{(n)}(\boldsymbol{v}) \right\}.$$

To bound the cardinality of this set, we introduce the following analogue of Definition 5.1:

Definition 5.2. *Let $\boldsymbol{R}, \boldsymbol{Q} \in \mathbb{Q}(\boldsymbol{X})^m$. We say that the iterations of $\boldsymbol{R}$ and $\boldsymbol{Q}$* generically escape each other *if, for every $k \in \mathbb{N}$, the k-th iterations of $\boldsymbol{R}$ and $\boldsymbol{Q}$ are well-defined and the set*

$$\left\{ \boldsymbol{w} \in \mathbb{C}^m \mid \boldsymbol{R}^{(k)}(\boldsymbol{w}) = \boldsymbol{Q}^{(k)}(\boldsymbol{w}) \right\}$$

is finite.

5.2. **Systems of rational functions.** We present our results in a simplified form where all constants depend on subsets of the following vector of parameters

$$\boldsymbol{\rho} = (d, D, h, H, m, s). \tag{5.2}$$

Consequently, in our results we use the notation '$O_{\boldsymbol{\rho}}$' and '$\ll_{\boldsymbol{\rho}}$', meaning that the implied constants do not depend on the parameters ε and N.

We also recall the definition of $T(\boldsymbol{w})$ given by (5.1).

Theorem 5.3. *Let $\boldsymbol{R} = (R_1, \ldots, R_m)$ be a system of $m \geq 2$ rational functions in $\mathbb{Q}(\boldsymbol{X})$ of degree at most $d \geq 2$ and of height at most h. Let $P_1, \ldots, P_s \in \mathbb{Z}[\boldsymbol{X}]$ of degree at most D and height at most H, and denote by $V \subset \mathbb{A}_{\mathbb{Q}}^m$ the variety defined by this system of polynomials. Assume that the iterations of $\boldsymbol{R}$ generically escape V. Then, there is a constant $c(\boldsymbol{\rho}) > 0$ such that for any real $\varepsilon > 0$ and $N \in \mathbb{N}$ with*

$$N \geq \exp\left(\frac{c(\boldsymbol{\rho})}{\varepsilon}\right), \tag{5.3}$$

there exists $\mathfrak{B} \in \mathbb{N}$ with

$$\log \mathfrak{B} \leq \exp\left(\frac{c(\boldsymbol{\rho})}{\varepsilon}\right)$$

such that, if p is a prime number not dividing $\mathfrak{B}$, then for any $\boldsymbol{w} \in \overline{\mathbb{F}}_p^m$ with $T(\boldsymbol{w}) \geq N$,

$$\frac{\#\mathfrak{V}_{\boldsymbol{w}}(\boldsymbol{R}, V; p, N)}{N} \leq \varepsilon.$$

We derive from Theorem 5.3 the following bound for the number of orbit intersection for two systems of rational functions.

Corollary 5.4. *Let $\boldsymbol{R} = (R_1, \ldots, R_m)$ and $\boldsymbol{Q} = (Q_1, \ldots, Q_m)$ be two systems of rational functions in $\mathbb{Q}(\boldsymbol{X})$ of degree at most d and of height at most h such that their iterations generically escape each other. Then* *there is a constant $c(\boldsymbol{\rho}) > 0$ such that, for any real $\varepsilon > 0$ and $N \in \mathbb{N}$ with*

$$N \geq \exp\left(\frac{c(\boldsymbol{\rho})}{\varepsilon}\right),$$

there exists $\mathfrak{B} \in \mathbb{N}$ with

$$\log \mathfrak{B} \leq \exp\left(\frac{c(\boldsymbol{\rho})}{\varepsilon}\right)$$

such that, if p is a prime number not dividing $\mathfrak{B}$, then for any $\boldsymbol{u}, \boldsymbol{v} \in \overline{\mathbb{F}}_p^m$ with $T(\boldsymbol{u}), T(\boldsymbol{v}) \geq N$,

$$\frac{\#\mathfrak{I}_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{R}, \boldsymbol{Q}; p, N)}{N} \leq \varepsilon.$$

Remark 5.5. *Alternatively, the bounds in Theorem 5.3 and Corollary 5.4 can be formulated taking ε as a function of p. More precisely, for some constant $c_0(\boldsymbol{\rho}) > 0$, one can take*

- *$\varepsilon = c_0(\boldsymbol{\rho})/\log\log p$ for any prime p and eliminate any influence of $\mathfrak{B}$. Since $\mathfrak{B} \leq \exp\exp(c(\boldsymbol{\rho})\varepsilon^{-1})$, the condition $p \nmid \mathfrak{B}$ is automatically satisfied for such ε, provided that $c_0(\boldsymbol{\rho})$ is large enough;*
- *$\varepsilon = c_0(\boldsymbol{\rho})/\log Q$ for all but $o(Q/\log Q)$ primes $p \leq Q$, since $\mathfrak{B}$ has at most $\log \mathfrak{B} \leq \exp(c(\boldsymbol{\rho})\varepsilon^{-1})$ prime divisors.*

Remark 5.6. *For systems with slower than generic growth of the degree and height the bounds in Theorem 5.3 and Corollary 5.4 can be improved. Some examples of such systems are given in §7.*

5.3. **Preparation.** We need the following simple combinatorial statement.

Lemma 5.7. *Let $2 \leq M < N/2$. For any sequence*

$$0 \leq n_1 < \ldots < n_M \leq N,$$

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

Proof. We denote by $I(s)$ the number of $i = 1, \ldots, M-1$ with $n_{i+1} - n_i = s$. Clearly

$$\sum_{s=1}^{N} I(s) = M - 1 \qquad \text{and} \qquad \sum_{s=1}^{N} I(s)s = n_M - n_1 \leq N.$$

Thus, for any integer $t \geq 1$ we have

$$\begin{aligned}\sum_{s=1}^{t} I(s) &= M - 1 - \sum_{s=t+1}^{N} I(h) \\ &\geq M - 1 - \frac{1}{t+1}\sum_{s=t+1}^{N} I(s)s \geq M - 1 - \frac{1}{t+1}N.\end{aligned}$$

Hence, there exists $r \in \{1, \dots, t\}$ with

$$I(r) \geq \frac{1}{t}\sum_{s=1}^{t} I(s) \geq \frac{M-1-N/(t+1)}{t}. \tag{5.4}$$

We now set $t = \lfloor 2N/(M-1) \rfloor$. Clearly

$$1 \leq t \leq \frac{2N}{(M-1)} \qquad \text{and} \qquad \frac{N}{t+1} < \frac{M-1}{2}.$$

Hence

$$\frac{M-1-N/(t+1)}{t} \geq \frac{M-1}{2t} \geq \frac{(M-1)^2}{4N},$$

which together with (5.4) concludes the proof. □

5.4. **Proof of Theorem 5.3.** Let p be a prime and $n \in \mathbb{N}$. As at the beginning of this section, we denote by $\boldsymbol{R}_p^{(n)}$ and V_p the reduction modulo p of $\boldsymbol{R}^{(n)}$ and V, respectively. Fix an initial point $\boldsymbol{w} \in \overline{\mathbb{F}}_p^m$ and let $M \in \mathbb{N}$ be the number of values of $n \in \{0, \dots, N-1\}$ such that $\boldsymbol{R}_p^{(n)}(\boldsymbol{w}) \in V_p$.

Suppose that

$$M > \varepsilon N \geq 2. \tag{5.5}$$

Then take $r \leq 2N/(M-1)$ as in Lemma 5.7 and let $\mathcal{N}$ be the set of $n \in \{0, \dots, N-1\}$ with

$$\boldsymbol{R}_p^{(n)}(\boldsymbol{w}) \in V_p \qquad \text{and} \qquad \boldsymbol{R}_p^{(n+r)}(\boldsymbol{w}) = \boldsymbol{R}_p^{(r)}\left(\boldsymbol{R}_p^{(n)}(\boldsymbol{w})\right) \in V_p. \tag{5.6}$$

By Lemma 5.7,

$$\#\mathcal{N} \geq \frac{(M-1)^2}{4N} \gg \varepsilon^2 N. \tag{5.7}$$

By (5.5), we have $r \ll \varepsilon^{-1}$.

Since the iterations of $\boldsymbol{R}$ generically escape V, the set $\{\boldsymbol{z} \in V \mid \boldsymbol{R}^{(r)}(\boldsymbol{z}) \in V\}$ is finite. This set is defined by the following $2s+1$ equations

$$\begin{aligned} P_\nu(\boldsymbol{X}) = P_\nu\left(\boldsymbol{R}^{(r)}(\boldsymbol{X})\right) &= 0, \qquad \nu = 1, \dots, s, \\ 1 - X_0 \prod_{i=1}^{m} G_{i,r}(\boldsymbol{X}) &= 0 \end{aligned} \tag{5.8}$$

where, as in the proof of Theorem 4.2, we write

$$R_i^{(r)} = \frac{F_{i,r}}{G_{i,r}}, \qquad F_{i,r}, G_{i,r} \in \mathbb{Z}[\boldsymbol{X}],$$

with relative prime polynomials $F_{i,r}, G_{i,r} \in \mathbb{Z}[\boldsymbol{X}]$, and introduce one more variable X_0.

From now on, we denote by $c_i(\boldsymbol{\rho})$, $i = 1, 2, \dots$, a sequence of suitable constants depending only on the parameters in $\boldsymbol{\rho}$. By Bézout's theorem and the degree bounds of Lemmas 3.3 and 3.5 we have

$$\begin{aligned}
&\#\{\boldsymbol{z} \in V \mid \boldsymbol{R}^{(r)}(\boldsymbol{z}) \in V\} \\
&\qquad \le D^s (D d^r m^{r-1})^s ((d^r m^{r-1})^m + 1) \le \exp\left(\frac{c_1(\boldsymbol{\rho})}{\varepsilon}\right).
\end{aligned} \tag{5.9}$$

Using the height bound of Lemma 3.5, we also obtain

$$\mathrm{h}(\boldsymbol{R}_i^{(r)}) \le \exp\left(\frac{c_2(\boldsymbol{\rho})}{\varepsilon}\right), \qquad i = 1, \dots, m.$$

Therefore, by Lemma 3.3, clearing the denominators, we see that the $2s+1$ polynomials in (5.8) have degree and height of size bounded by $\exp(c_3(\boldsymbol{\rho})\varepsilon^{-1})$.

Hence, by Theorem 2.1, there is a positive integer $\mathfrak{B}$ with

$$\log \mathfrak{B} \le \exp\left(\frac{c_4(\boldsymbol{\rho})}{\varepsilon}\right)$$

such that, if $p \nmid \mathfrak{B}$, then

$$\#\{\boldsymbol{z} \in V_p \mid \boldsymbol{R}_p^{(r)}(\boldsymbol{z}) \in V_p\} = \#\{\boldsymbol{z} \in V \mid \boldsymbol{R}^{(r)}(\boldsymbol{z}) \in V\}.$$

Since $N \le T(\boldsymbol{w})$, the points $\boldsymbol{R}_p^{(n)}(\boldsymbol{w})$, $n = 0, \dots, N-1$, are pairwise distinct. Hence,

$$\#\mathcal{N} \le \#\{\boldsymbol{z} \in V_p \mid \boldsymbol{R}_p^{(r)}(\boldsymbol{z}) \in V_p\}.$$

From (5.6), (5.7) and (5.9) we deduce that

$$\varepsilon^2 N \le \exp\left(\frac{c_1(\boldsymbol{\rho})}{\varepsilon}\right).$$

Choosing $c(\boldsymbol{\rho}) = \max\{c_4(\boldsymbol{\rho}), c_1(\boldsymbol{\rho}) + 1\}$, this contradicts (5.3). Hence $M \le \varepsilon N$ and the result follows.

5.5. **Proof of Corollary 5.4.** If $\mathfrak{I}_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{R}, \boldsymbol{Q}; p, N)$ is empty, the statement is trivial. Otherwise, let $n_0 \in \mathbb{N}$ be the smallest element in this set. Then

$$\#\mathfrak{I}_{\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{R}, \boldsymbol{Q}; p, N) = \#\mathfrak{I}_{\boldsymbol{w},\boldsymbol{w}}(\boldsymbol{R}, \boldsymbol{Q}; p, N - n_0)$$

with $\boldsymbol{w} = \boldsymbol{R}^{(n_0)}(\boldsymbol{u})$. Moreover,

$$\mathfrak{I}_{\boldsymbol{w},\boldsymbol{w}}(\boldsymbol{R}, \boldsymbol{Q}; p, N - n_0) = \mathfrak{V}_{\boldsymbol{w}}((\boldsymbol{R}(\boldsymbol{X}), \boldsymbol{Q}(\boldsymbol{Y})), V; p, N - n_0)$$

for the $2m$-dimensional system of rational functions

$$(\boldsymbol{R}(\boldsymbol{X}), \boldsymbol{Q}(\boldsymbol{Y})) = (R_1(\boldsymbol{X}), \dots, R_m(\boldsymbol{X}), Q_1(\boldsymbol{Y}), \dots, Q_m(\boldsymbol{Y})),$$

and the variety V defined by the polynomials

$$P_j = X_j - Y_j, \qquad j = 1, \dots, m.$$

The hypothesis that the orbits of $\boldsymbol{R}$ and $\boldsymbol{Q}$ generically escape each other implies that the system $(\boldsymbol{R}(\boldsymbol{X}), \boldsymbol{Q}(\boldsymbol{Y}))$ generically escapes the variety V. The statement then follows from Theorem 5.3.

5.6. **Examples of iterations generically escaping a variety.** Clearly, the problem of finding nontrivial pairs $(\boldsymbol{R}, V)$ consisting of a system $\boldsymbol{R}$ of rational functions with iterations that generically escape a variety V is interesting in its own. Here we give a family of examples of this kind, as an application of a result of Dvir, Kollár and Lovett [DKL14, Theorem 2.1].

Let $m = 2s$ be even and let

$$A = (a_{i,j})_{i,j} \in \mathbb{Z}^{s\times m}$$

be an $s \times m$ matrix with integer entries such that any $s \times s$ minor is nonsingular. For instance, one may construct such a matrix as a Vandermonde or Cauchy matrix.

We now choose $2m$ positive integers with

$$d_1 > \ldots > d_m \qquad \text{and} \qquad e_1 > \ldots > e_m > d_1^s \tag{5.10}$$

such that $\gcd(d_ie_i, d_je_j) = 1$, $1 \le i, j \le m$, $i \ne j$.

We consider the monomial system $\boldsymbol{F} = (X_1^{e_1}, \ldots, X_m^{e_m}) \in \mathbb{Z}[\boldsymbol{X}]^m$ and the variety $V \subset \mathbb{C}^m$ defined by the s polynomials

$$P_j = \sum_{i=1}^{m} a_{j,i} X_i^{d_i}, \qquad j = 1, \ldots, s.$$

This variety is a complete intersection of degree at most d_1^s.

For any point $\boldsymbol{w} \in \mathbb{C}^m$ we have $\big(\boldsymbol{w}, \boldsymbol{F}^{(k)}(\boldsymbol{w})\big) \in V(\mathbb{C}) \times V(\mathbb{C})$ if and only if $\boldsymbol{w} \in U_k \cap V$, where U_k is the variety defined by the polynomials

$$P_j(X_1^{e_1^k}, \ldots, X_m^{e_m^k}) = \sum_{i=1}^{m} a_{j,i} X_i^{d_i e_i^k}, \qquad j = 1, \ldots, s.$$

As V is of dimension $m - s = s$, and recalling the conditions (5.10), we see that

$$d_1 e_1^k > \ldots > d_m e_m^k > d_1^s \ge \deg V.$$

Therefore, [DKL14, Theorem 2.1] applies and yields the finiteness of $U_k \cap V$. Hence, the iterations of the monomial system $\boldsymbol{F}$ generically escape the variety V, as desired.

6. Orbits on Varieties under the Uniform Dynamical Mordell-Lang Conjecture

6.1. **Varieties satisfying the uniform dynamical Mordell–Lang conjecture.** Informally, the dynamical Mordell–Lang conjecture asserts that the intersection of an orbit of an algebraic dynamical system (in affine or projective space over a field of zero characteristic) with a given variety is a union of a finite "sporadic" set and finitely many arithmetic progressions. Among other sources, this conjecture stems from the celebrated *Skolem-Mahler-Lech theorem* [BL13].

Here we consider a class of algebraic dynamical systems and varieties that satisfy the following stronger uniform condition.

Definition 6.1. *Let $\boldsymbol{R} \in \mathbb{Q}(\boldsymbol{X})^m$ be a system of rational functions over K and $V \subset \mathbb{A}^m_{\mathbb{Q}}$ an affine variety. The intersection of the orbits $\boldsymbol{R}$ with V is L-*uniformly bounded *if there is a constant L depending only on $\boldsymbol{R}$ and V such that for all initial values $\boldsymbol{w} \in \overline{\mathbb{Q}}^m$,*

$$\#\left\{n \in \mathbb{N} \mid \boldsymbol{w}_n \in V(\overline{\mathbb{Q}})\right\} \leq L,$$

with $\boldsymbol{w}_n$ is as in (2.2).

In this section, we reconsider the problem of §5 of bounding the number of elements in an orbit of a given system of rational functions lying in a variety satisfying this uniformity condition.

The boundedness of the number of orbit elements that fall in a variety, or more specialised questions of orbit intersections (see §5.5 where this link is made explicit), has recently been an object of active study, see [BGT14, BGKT10, BGKT12, GTZ08, GTZ12, OS15, SV13] and the references therein. Although we believe that the L-uniformly boundedness condition is generically satisfied, proving it for general classes of systems appear to be difficult.

6.2. **Systems of rational functions.** Here we add one parameter L in the definition of $\boldsymbol{\rho}$, so instead of (5.2) it is now given by

$$\boldsymbol{\rho} = (d, D, h, H, L, m, s).$$

We also continue to use $T(\boldsymbol{w})$ as given by (5.1). We obtain the following result which is a version of Theorem 5.3.

Theorem 6.2. *Let $\boldsymbol{R} = (R_1, \ldots, R_m)$ be a system of $m \geq 2$ rational functions in $\mathbb{Q}(\boldsymbol{X})$ of degree at most $d \geq 2$ and of height at most h. Let V be the affine algebraic variety defined by the polynomials $P_1, \ldots, P_s \in \mathbb{Z}[\boldsymbol{X}]$ of degree at most D and height at most H. We also assume that the intersection of orbits of $\boldsymbol{R}$ with V is L-uniformly bounded. There is a constant $c(\boldsymbol{\rho}) > 0$ such that, for any real $\varepsilon > 0$, there exists $\mathfrak{B} \in \mathbb{N}$ with*

$$\log \mathfrak{B} \leq \exp\left(\frac{c(\boldsymbol{\rho})}{\varepsilon}\right)$$

such that, if p is a prime number not dividing $\mathfrak{B}$, then for any integer

$$N \geq \frac{2L}{\varepsilon} + 1$$

and any initial point $\boldsymbol{w} \in \overline{\mathbb{F}}_p^m$ with $T(\boldsymbol{w}) \geq N$, we have

$$\frac{\#\mathfrak{V}_{\boldsymbol{w}}(\boldsymbol{R}, V; p, N)}{N} \leq \varepsilon.$$

Remark 6.3. *One can check that appropriate versions of Remarks 5.5 and 5.6 apply to Theorem 6.2 as well.*

6.3. **Proof of Theorem 6.2.** We set

$$M = \lfloor 2\varepsilon^{-1}L \rfloor + 1,$$

thus in particular $N \geq M$.

For each set $\mathcal{L} \subseteq \{0, \dots, M-1\}$ of cardinality $\#\mathcal{L} = L + 1$ we consider the system of equations

$$P_j(\boldsymbol{R}^{(k)}) = P_j\left(\frac{F_{1,k}}{G_{1,k}}, \dots, \frac{F_{m,k}}{G_{m,k}}\right) = 0, \qquad k \in \mathcal{L}, \ j = 1, \dots, s.$$

Let X_0 be an additional variable, set

$$\Gamma_{0,k} = 1 - X_0 \prod_{i=1}^{m} \prod_{j=1}^{k} G_{i,j}$$

and let $\Gamma_{j,k}$ be the numerator of $P_j(\boldsymbol{R}^{(k)})$. We now study the following system of equations in $m+1$ variables:

$$\Gamma_{j,k} = 0, \qquad k \in \mathcal{L}, \ j = 0, \dots, s. \tag{6.1}$$

By Lemmas 3.3 and 3.5, we have

$$\deg \Gamma_{0,k} \leq 2d^k m^k \qquad \text{and} \qquad \deg \Gamma_{j,k} \leq d^k D m^k,$$

which we combine in one bound

$$\deg \Gamma_{j,k} \leq d^k D m^k + 1, \qquad j = 0, \dots, s. \tag{6.2}$$

Also, by Lemmas 3.1 and 3.5, exactly as in the proof of Theorem 4.2, we have

$$\mathrm{h}(\Gamma_{0,k}) \ll_{\boldsymbol{\rho}} (dm)^k. \tag{6.3}$$

By Lemmas 3.3 and 3.5 again, we also have

$$\begin{aligned}\mathrm{h}(\Gamma_{j,k}) \leq H + Dh &\left(1 + d\frac{d^{k-1}m^{k-1} - 1}{dm - 1}\right) \\ &+ dD(3dm+1)\frac{d^{k-1}m^{k-1} - 1}{dm - 1}\log(m+1) \\ &+ D(3d^k m^k + 1)\log(m+1) \ll_{\boldsymbol{\rho}} (dm)^k.\end{aligned} \tag{6.4}$$

For simplicity, we use the bound (6.4) also for $\mathrm{h}(\Gamma_{0,k})$, even if we loose slightly in the final bound.

By the assumption on $\boldsymbol{R}$ and L, the equations (6.1) have no common solution $\boldsymbol{w} \in \overline{\mathbb{Q}}^m$. By Theorem 2.1 together with the bounds (6.2), (6.3) and (6.4) and the fact that $k \leq M - 1$, there exists $\mathfrak{A}_{\mathcal{L}} \in \mathbb{N}$ with

$$\log \mathfrak{A}_{\mathcal{L}} \ll_{\boldsymbol{\rho}} (d^{M-1} D m^{M-1} + 1)^{3(m+1)+2}$$

such that, if p is a prime not dividing $\mathfrak{A}_{\mathcal{L}}$, then the reduction modulo p of the system of equations (6.1) has no solution in $\overline{\mathbb{F}}_p^m$.

We now set

$$\mathfrak{B} = \prod_{\substack{\mathcal{L}\subseteq\{0,\ldots,M-1\} \\ \#\mathcal{L}=L+1}} \mathfrak{A}_{\mathcal{L}}$$

and note that $\mathfrak{B} \geq 1$

$$\log \mathfrak{B} \ll_{\boldsymbol{\rho}} \binom{M}{L+1} (d^{M-1}Dm^{M-1}+1)^{3(m+1)+2} \leq \exp\left(\frac{c_1(\boldsymbol{\rho})}{\varepsilon}\right) \tag{6.5}$$

for a constant $c_1(\boldsymbol{\rho})$.

Let p be a prime with $p \nmid \mathfrak{B}$. Suppose that for some $\boldsymbol{u} \in \overline{\mathbb{F}}_p^m$ there are at least εN values of $n \in \{0,\ldots,N-1\}$ with $\boldsymbol{R}_p^{(n)}(\boldsymbol{u}) \in V_p$. We recall that $N \geq M$, so $\lfloor N/M \rfloor + 1 \leq 2N/M$. Therefore, there is a nonnegative integer $i \leq \lfloor N/M \rfloor$ such that there are at least

$$\frac{\varepsilon N}{\lfloor N/M \rfloor + 1} \geq \frac{1}{2}\varepsilon M > L$$

values of $n \in \{iM,\ldots,(i+1)M-1\}$ with $\boldsymbol{R}_p^{(n)}(\boldsymbol{u}) \in V_p$. Take $L+1$ such values and write them as

$$s < s+t_1 < \ldots < s+t_{L+1} < s+M$$

where $s = iM$. Then, for $j = 1,\ldots,s$ and $\nu = 1,\ldots,L+1$,

$$P_j\left(\boldsymbol{R}_p^{(t_\nu)}\left(\boldsymbol{R}_p^{(s)}(\boldsymbol{u})\right)\right) = 0.$$

So, setting $\boldsymbol{w} = \boldsymbol{R}_p^{(s)}(\boldsymbol{u}) \in \overline{\mathbb{F}}_p$, we obtain

$$P_j\left(\boldsymbol{R}_p^{(t_\nu)}(\boldsymbol{w})\right) = 0$$

for all such j,ν. This implies that $p \mid \mathfrak{A}_{\mathcal{L}}$ with $\mathcal{L} = \{t_1,\ldots,t_{L+1}\}$, and thus we obtain a contradiction.

7. Some remarks

Clearly, our results depend on the growth of the degree and the height of the iterates (1.1). When this growth is slower than "generic", one can expect stronger bounds. For example, this is true for the following family of systems which stems from that introduced in [OS10], see also [GOS14, OS12].

For $i = 1,\ldots,m$, let

$$F_i \in \mathbb{Z}[X_i, X_{i+1},\ldots,X_m] \tag{7.1}$$

be a "triangular" system of polynomials F_i which do not depend on the first $i-1$ variables and with a term of the form $g_i X_i X_{i+1}^{s_{i,i+1}} \ldots X_m^{s_{i,m}}$ such that $g_i \in \mathbb{Z}\setminus\{0\}$, $\deg_{X_i} F_i = 1$ and $\deg_{X_j} F_i = s_{i,j}$, $j = i+1,\ldots,m$.

Using the same idea as in [OS10], similarly to the bounds of §3, one can show that for the systems (7.1) the degree and the height of the kth iterate grow polynomially and thus obtain stronger versions of our main results in §4, §5 and §6.

Indeed, an inductive argument shows that for any integer $k \geq 1$, the polynomials $F_i^{(k)}$, $i = 1, \ldots, m$, defined by (1.1), are of degree and height at most

$$d_{i,k} = O_{d,m}(k^{m-i}) \qquad \text{and} \qquad h_{i,k} = O_{d,h,m}(k^{m-i+2}).$$

In turn, one obtains a version of Theorem 4.3 with an integer $\mathfrak{A}_k \geq 1$ satisfying

$$\log \mathfrak{A}_k \ll_{d,h,m} k^{m(3m-1)}$$

and such that, if p is a prime number not dividing $\mathfrak{A}_k$, then the reduction of $\boldsymbol{F}$ modulo p has at most $O_{d,h,m}(k^{m(m-1)/2})$ periodic points of order k. Similarly, for systems the form (7.1) a version of Theorem 5.3 holds with

$$N \geq c(\boldsymbol{\rho})\varepsilon^{-(m-1)s-2} \qquad \text{and} \qquad \log \mathfrak{B} \leq c(\boldsymbol{\rho})\varepsilon^{-m(3m-1)},$$

while a version of Theorem 6.2 holds with

$$\log \mathfrak{B} \leq c(\boldsymbol{\rho})\varepsilon^{-(m-1)s(L+1)+m+L+1}$$

and the same value of N.

The polynomial systems of the form (7.1) have been generalised in various directions, including their rational function analogues [GOS14, HP07]. It is expected that similar improvements hold for all these systems as well.

References

[AG09] A. Akbary and D. Ghioca, 'Periods of orbits modulo primes', *J. Number Theory* **129** (2009), 2831–2842. (pp. 2 and 20)

[AK09] V. Anashin and A. Khrennikov, *Applied algebraic dynamics*, Walter de Gruyter, 2009. (p. 1)

[BGT14] J. P. Bell, D. Ghioca and T. J. Tucker, 'The dynamical Mordell-Lang problem', Math. Surveys and Monographs, vol. 210, Amer. Math. Soc., Providence, RI, 2016, (p. 29)

[BL13] J. P. Bell and J. Lagarias, 'A Skolem-Mahler-Lech theorem for iterated automorphisms of K-algebras', *Canad. J. Math.*, **67** (2015), 286–314. (p. 29)

[BGKT10] R. L. Benedetto, D. Ghioca, P. Kurlberg and T. J. Tucker, 'A gap principle for dynamics', *Compositio Math.* **146** (2010), 1056–1072. (p. 29)

[BGKT12] R. L. Benedetto, D. Ghioca, P. Kurlberg and T. J. Tucker, 'A case of the dynamical Mordell- Lang conjecture (with an Appendix by U. Zannier)', *Math. Ann.* **352** (2012), 1–26. (p. 29)

[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. (p. 2)

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge Univ. Press, 2006. (p. 9)

[CDO+18] M.-C. Chang, C. D'Andrea, A. Ostafe, I. E. Shparlinski and M. Sombra, 'Orbits of polynomial dynamical systems modulo primes', *Proc. Amer. Math. Soc.*, **146** (2018), 2015–2025. (pp. 3 and 20)

[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. (pp. 2, 3, 9, 10, and 12)

[DKL14] Z. Dvir, J. Kollár and S. Lovett, 'Variety evasive sets', *Comput. Complexity* **23** (2014), 509–529. (p. 28)

[GTZ08] D. Ghioca, T. Tucker and M. Zieve, 'Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture', *Invent. Math.* **171** (2008), 463–483. (pp. 22 and 29)

[GTZ12] D. Ghioca, T. Tucker and M. Zieve, 'Linear relations between polynomial orbits', *Duke Math. J.* **161** (2012), 1379–1410. (pp. 22 and 29)

[GOS14] D. Gómez-Pérez, A. Ostafe and I. E. Shparlinski, 'Algebraic entropy, automorphisms and sparsity of algebraic dynamical systems and pseudorandom number generators', *Math. Comp.* **83** (2014), 1535–1550. (pp. 31 and 32)

[HMPS00] K. Hägele, J. E. Morais, L. M. Pardo and M. Sombra, 'On the intrinsic complexity of the arithmetic Nullstellensatz', *J. Pure Appl. Algebra.* **146** (2000), 103–183. (p. 2)

[HP07] B. Hasselblatt and J. Propp, 'Degree growth of monomial maps', *Ergodic Theory Dynam. Systems* **27** (2007), 1375–1397. (p. 32)

[Jon08] R. Jones, 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials', *J. Lond. Math. Soc.* **78** (2008), 523–544. (p. 2)

[Koi96] P. Koiran, 'Hilbert's Nullstellensatz is in the polynomial hierarchy', *J. Complexity* **12** (1996), 273–286. (p. 2)

[KPS01] T. Krick, L. M. Pardo, and M. Sombra, 'Sharp estimates for the arithmetic Nullstellensatz', *Duke Math. J.* **109** (2001), 521–598. (pp. 2, 3, 10, 13, and 16)

[Liu02] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Grad. Texts in Math., vol. 6, Oxford Univ. Press, 2002. (pp. 5, 6, and 7)

[Nes77] Yu. V. Nesterenko, 'Estimates for the orders of zeros of functions of a certain class and applications in the theory of transcendental numbers', *Izv. Akad. Nauk SSSR Ser. Mat.* **41** (1977), 253–284. (pp. 7 and 8)

[OS15] A. Ostafe and M. Sha, 'On the quantitative dynamical Mordell-Lang conjecture', *J. Number Theory* **156** (2015), 161–182. (p. 29)

[OS10] A. Ostafe and I. E. Shparlinski, 'On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators', *Math. Comp.* **79** (2010), 501–511. (p. 31)

[OS12] A. Ostafe and I. E. Shparlinski, 'Degree growth, linear independence and periods of a class of rational dynamical systems', *Arithmetic, Geometry, Cryptography and Coding Theory 2010*, Contemp. Math., vol. 574, Amer. Math. Soc., 2012, pp. 131–143. (p. 31)

[Phi86] P. Philippon, 'Critères pour l'indépendance algébrique', *Inst. Hautes tudes Sci. Publ. Math.* **64** (1986), 5–52. (pp. 7 and 8)

[PS08] P. Philippon and M. Sombra, 'Hauteur normalisée des variétés toriques projectives', *J. Inst. Math. Jussieu* **7** (2008), 327–373. (p. 9)

[RV09] J. A. G. Roberts and F. Vivaldi, 'A combinatorial model for reversible rational maps over finite fields', *Nonlinearity* **22** (2009), 1965–1982. (p. 2)

[Sch95] K. Schmidt, *Dynamical systems of algebraic origin*, Progress in Math., vol. 128, Birkhäuser Verlag, 1995. (p. 1)

[Sil07] J. H. Silverman, *The arithmetic of dynamical systems*, Springer Verlag, 2007. (pp. 1 and 3)

[Sil08] J. H. Silverman, 'Variation of periods modulo p in arithmetic dynamics', *New York J. Math.* **14** (2008), 601–616. (pp. 2 and 20)

[SV13] J. H. Silverman and B. Viray, 'On a uniform bound for the number of exceptional linear subvarieties in the dynamical Mordell-Lang conjecture', *Math. Res. Letters* **20** (2013), 547–566. (p. 29)

[Som04] M. Sombra, 'The height of the mixed sparse resultant', *Amer. J. Math.* **126** (2004), 1253–1260. (p. 14)

[Tow13] A. Towsley, 'A Hasse principle for periodic points', *Intern. J. Number Theory* **8** (2013), 2053–2068. (p. 2)

Departament de Matemàtiques i Informàtica, Universitat de Barcelona (UB). Gran Via 585, 08007 Barcelona, Spain

E-mail address: cdandrea@ub.edu

URL: http://www.ub.edu/arcades/cdandrea.html

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. Passeig Lluís Companys 23, 08010 Barcelona, Spain

Departament de Matemàtiques i Informàtica, Universitat de Barcelona (UB). Gran Via 585, 08007 Barcelona, Spain

E-mail address: sombra@ub.edu

URL: http://www.maia.ub.es/~sombra/