PERIODS OF ORBITS MODULO PRIMES

AMIR AKBARY AND DRAGOS GHIOCA

Abstract. Let S be a monoid of endomorphisms of a quasiprojective variety V defined over a global field K. We prove a lower bound for the size of the reduction modulo places of K of the orbit of any point $\alpha \in V(K)$ under the action of the endomorphisms from S. We also prove a similar result in the context of Drinfeld modules. Our results may be considered as dynamical variants of Artin's primitive root conjecture.

1. Introduction

Artin's primitive root conjecture asserts that if $a \in \mathbb{Z}$ and $a \neq -1$ or a square, then the set of primes p for which $a \pmod p$ is a primitive root has positive density. Pappalardi [20] and Erdös and R. Murty [8] proved variants of Artin's conjecture for finitely generated subgroups of $\mathbb{Q}^*$. More precisely, it is proved in [20] that for a subgroup Γ of rank $r \geq 1$ of $\mathbb{Q}^*$, the set of primes p, for which the reduction Γ_p of Γ modulo p has less than $p^{\frac{r}{r+1}}$ elements, has natural density 0. More precisely, Pappalardi proved that for all but $o(x/\log x)$ primes $p \leq x$, we have

$$|\Gamma_p| \geq p^{\frac{r}{r+1}} \exp\left(\log^{\tau} p\right) \text{ for some } \tau \sim 0.15.$$

Similar results were proved for finitely generated subgroups of elliptic curves (see [13], [1]) and for finitely generated subgroups of arbitrary algebraic groups (see [16]).

There are two dynamical interpretations of these results. Firstly, each finitely generated subgroup Γ of $\mathbb{Q}^*$ may be viewed as the image of $1 \in \mathbb{Q}^*$ under the subgroup S of automorphisms of $\mathbb{G}_m/\mathbb{Q}$ generated by the finitely many translation maps given by $x \mapsto a_i \cdot x$, where $a_1, \ldots, a_r$ is an arbitrary (finite) set of generators for Γ. Denoting by $\mathcal{O}^S(1)$ the orbit of $1 \in \mathbb{G}_m(\mathbb{Q})$ under the maps from S, the results of Pappalardi, Erdös and R. Murty offer information about the size of the reduction of $\mathcal{O}^S(1)$ modulo various primes p. Similarly, the results for Artin's conjecture in the context of elliptic curves can be phrased in terms of orbits under subgroups of automorphisms generated by finitely many translation maps. In this paper, we replace S by a monoid generated by finitely many endomorphisms of an arbitrary quasiprojective variety V defined over a global field (see Section 2).

We state below a special case of our results when S is a cyclic monoid (see Section 2 for our general setup, and also Theorems 2.1 and 2.3 for our more general results). In order to state Theorem 1.1 we define the degree of an endomorphism.

Let $V \subset \mathbb{P}^M$ be a quasiprojective variety defined over a field K, and let $\Phi : V \longrightarrow V$ be an endomorphism defined over K. Thus V is a finite union of Zariski open subsets V_ℓ of projective subvarieties of $\mathbb{P}^M$ such that $\Phi_\ell := \Phi \mid_{V_\ell}$ can be written as $[F_{\ell 0} : \cdots : F_{\ell M}]$, where the $F_{\ell i}$ are

2000 *Mathematics Subject Classification.* Primary: 11G35, 11G50; Secondary: 14G40, 37F10.

Key words and phrases. Artin's conjecture, algebraic dynamics, Drinfeld modules.

Research of both authors was partially supported by NSERC.

relatively prime homogeneous polynomials of degree d_ℓ which do not vanish simultaneously on V_ℓ; hence we may view Φ_ℓ as a rational map on $\mathbb{P}^M$ of degree d_ℓ. We define the *degree* of Φ as

$$\deg(\Phi) := \max_\ell d_\ell.$$

For any endomorphism Φ of V, and for any $\alpha \in V$, we let $\mathcal{O}^{\langle\Phi\rangle}(\alpha)$ be the Φ-orbit of α, i.e. the set of all $\Phi^n(\alpha)$ for $n \in \mathbb{N}$ (where by Φ^n we denote the n-th iterate of Φ, and as always $\mathbb{N}$ denotes the set of nonnegative integers). Also, in general, we denote by $\langle\Phi\rangle$ the monoid (semigroup with identity) generated by Φ.

Theorem 1.1. *Let V be a quasiprojective variety defined over a global field K, and let $\Phi : V \longrightarrow V$ be an endomorphism of V defined over K. Let $\alpha \in V(K)$ be a nonpreperiodic point for Φ (i.e., the Φ-orbit $\mathcal{O}^{\langle\Phi\rangle}(\alpha)$ of α is infinite). We have*

(i) If $\deg(\Phi) > 1$ then for each $\epsilon < 1/\log\deg(\Phi)$, the natural density of the set of places v of K for which the reduction of $\mathcal{O}^{\langle\Phi\rangle}(\alpha)$ modulo v has less than $\epsilon\log \mathrm{N}(v)$ elements equals zero (where $\mathrm{N}(v)$ represents the size of the residue field modulo v).

(ii) If $\deg(\Phi) = 1$ then for each $\gamma < 1/2$, the natural density of the set of places v of K for which the reduction of $\mathcal{O}^{\langle\Phi\rangle}(\alpha)$ modulo v has less than $\mathrm{N}(v)^\gamma$ elements equals zero.

Remark 1.2. Actually, we prove a stronger statement, i.e., for each $x > 0$, the set of places v of K such that $\mathrm{N}(v) \le x$ which do not satisfy (i) or (ii) is less than $\pi(x)^\alpha$ for some $\alpha < 1$, where $\pi(x)$ is the number of *all* places v of K satisfying $\mathrm{N}(v) \le x$.

The area of algebraic dynamics was pioneered by Northcott (see [19]); later, Silverman (see [24] for a comprehensive treatment of this subject) greatly developed all aspects of the theory of algebraic dynamics. Silverman [23], and Call and Silverman [5] constructed canonical heights associated to polarizable endomorphisms of general varieties, which gave rise to several directions of research in algebraic dynamics (see [17, 18], for example). Later, Zhang [27] proposed a series of conjectures for algebraic dynamical systems, many of which are natural analogs of classical theorems for abelian varieties. Recently, various authors proved a number of new algebraic dynamic results; these include equidistribution results (see [2, 6, 9]), and analogs of the Mordell-Lang and the Bogomolov conjectures (see [11, 3, 4, 10]).

In [25] Silverman proved a weaker version of the above Theorem 1.1 for number fields; this constituted the inspiration for our present paper. More precisely, for a number field K, he proved the following result ([25, Theorem 2]).

Theorem 1.3 (Silverman). *Let $K/\mathbb{Q}$ be a number field with the ring of integers R_K and let V, Φ and $\mathcal{O}^{\langle\Phi\rangle}(\alpha)$ be as described in part (i) of Theorem 1.1. Let $\mathfrak{p}$ denote any nonzero prime ideal of R_K and $N(\mathfrak{p})$ denote the norm of $\mathfrak{p}$. We have*

(a) For each $\gamma < 1$, the logarithmic analytic density of the set of prime ideals $\mathfrak{p}$ of R_K for which the reduction of $\mathcal{O}^{\langle\Phi\rangle}(\alpha)$ modulo $\mathfrak{p}$ has less than $(\log N(\mathfrak{p}))^\gamma$ elements equals zero.

(b) There is a constant $C = C(K, V, \Phi, \alpha)$ so that for all $\epsilon > 0$ the upper logarithmic analytic density of the set of prime ideals $\mathfrak{p}$ of R_K for which the reduction of $\mathcal{O}^{\langle\Phi\rangle}(\alpha)$ modulo $\mathfrak{p}$ has less than $\epsilon\log N(\mathfrak{p})$ elements, is less than $C\epsilon$.

Recall that all but finitely many places of a number field K correspond to non-zero prime ideals of R_K. Also note that for each $\epsilon > 0$ and for each $\gamma < 1$, for all but finitely many prime ideals $\mathfrak{p}$, we have $(\log \mathrm{N}(\mathfrak{p}))^\gamma < \epsilon \log \mathrm{N}(\mathfrak{p})$. So part (i) of Theorem 1.1 implies part (a) of Silverman's result as a set with natural density zero has also logarithmic analytic density zero (see [26, Chapter III.1]). Moreover, if $\epsilon < 1/\log\deg(\Phi)$, part (i) of Theorem 1.1 leads to a stronger result than part (b) of Theorem 1.3.

In Theorems 2.1 and 2.3 we generalize the result of Theorem 1.1 to the case of orbits under a monoid generated by finitely many endomorphisms of V.

A second interpretation of the results of Pappalardi, Erdös and R. Murty on Artin's primitive root conjecture is as follows. We let $\rho : (\mathbb{Z}, +, \cdot) \longrightarrow (\mathrm{End}(\mathbb{G}_m/\mathbb{Q}), \cdot, \circ)$ be the usual $\mathbb{Z}$-algebra homomorphism such that $\rho_k := \rho(k)$ is the k-th power map for each integer k, i.e. $\rho_k(x) = x^k$ for any x. Hence $\mathbb{Z}$ acts on $\mathbb{G}_m(\mathbb{Q})$ through the endomorphisms induced by ρ. Then each finitely generated subgroup $\Gamma \subset \mathbb{Q}^*$ may be viewed as the finitely generated $\mathbb{Z}$-module, under the action of ρ, generated by some $x_1, \dots, x_r \in \mathbb{Q}^*$, and thus we are interested in the size of the reduction of this $\mathbb{Z}$-module modulo various primes. We can develop a similar construction for the additive group scheme $\mathbb{G}_a/K$ where K is a global field. We observe that in characteristic p any finitely generated submodule of the additive group considered as a $\mathbb{Z}$-module is finite and so the size of the reduction of such submodule is uniformly bounded. So for the correct setting, in characteristic p, we should consider $\mathbb{G}_a/K$ as an $\mathbb{F}_p[t]$-module. In Section 5 we consider such construction which is described naturally in the context of Drinfeld modules. Indeed, each Drinfeld module defined over a function field K (of characteristic p) corresponds to a ring homomorphism $\rho : (\mathbb{F}_p[t], +, \cdot) \longrightarrow (\mathrm{End}(\mathbb{G}_a/K), +, \circ)$, and thus we are interested in the size of the reduction modulo various primes of a finitely generated $\mathbb{F}_p[t]$-module under the action of ρ. We prove the following result (see Section 5 for more details about Drinfeld modules).

Theorem 1.4. *(i) Let K be a finite extension of $\mathbb{F}_p(t)$, and let $\rho : \mathbb{F}_p[t] \longrightarrow \mathrm{End}(\mathbb{G}_a/K)$ be a Drinfeld module of rank n. Let $\Gamma \subset K$ be a free $\mathbb{F}_p[t]$-submodule of rank $r \geq 1$ under the action of ρ. Then for each $\gamma < r/(n+r)$, the natural density of the set of places v of K such that the reduction of Γ modulo v has less than $\mathrm{N}(v)^\gamma$ elements equals zero.*

(ii) Let K be a global field. Let $A = \mathbb{Z}$, if the characteristic of K is zero, and $A = \mathbb{F}_p[t]$, if the characteristic of K is p. Let $\rho : A \longrightarrow \mathrm{End}(\mathbb{G}_a/K)$ be such that $\rho_a(x) = a \cdot x$ for each $a \in A$, and for each $x \in K$. Let $\Gamma \subset K$ be a nontrivial A-submodule under the action of ρ. Then for each $\gamma < 1$, the natural density of the set of places v of K such that the reduction of Γ modulo v has less than $\mathrm{N}(v)^\gamma$ elements equals zero.

Because each Drinfeld module $\rho : \mathbb{F}_p[t] \longrightarrow \mathrm{End}(\mathbb{G}_a/K)$ induces a dynamical system on the affine line, the proof of Theorem 1.4 is similar with the proof of Theorem 1.1; however, because $(\mathbb{F}_p[t], \cdot)$ is not finitely generated, no cyclic $\mathbb{F}_p[t]$-module under the action of ρ, may be represented as the orbit $\mathcal{O}^S(\alpha)$ of a point α under a finitely generated monoid S of endomorphisms of the affine line. More precisely, if S is generated by any finite subset of maps $\rho_{f(t)} := \rho(f(t))$ (for some $f(t) \in \mathbb{F}_p[t]$), then $\mathcal{O}^S(\alpha)$ is a proper subset of the cyclic $\mathbb{F}_p[t]$-module generated by α under the action of ρ; this explains why the conclusion of our Theorem 1.4 is much stronger than the conclusion of its counterpart result from Theorem 1.1.

We sketch briefly the plan of our paper. In Section 2 we set the notation for our main result for arbitrary endomorphisms. We continue in Section 3 by stating basic properties of heights over global fields. Then we prove in Section 4 our main results for arbitrary endomorphisms of a quasiprojective variety (Theorems 2.1 and 2.3), while in Section 5 we prove our main result for Drinfeld modules (Theorem 5.2). Our main theorems are proved by using combinatorial arguments and the height inequalities of Section 3.

Acknowledgment. The authors would like to thank the referee for helpful suggestions.

2. Statement of our main results for arbitrary endomorphisms

A *global field* is either a number field or a function field of transcendence degree 1 over the prime field $\mathbb{F}_p$ (i.e., it is a finite extension of $\mathbb{F}_p(t)$). Let K be a global field; let R_K be the ring of algebraic integers of K (if K is a number field), or the integral closure of $\mathbb{F}_p[t]$ in K (if K is a function field). In both the number field case and the function field case, we say that R_K is the ring of integers of K; it is known that R_K is a Dedekind domain. If K is a function field, we let $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ inside K; we also call $\mathbb{F}_q$ the *constant field* of K.

By a *finite place* of K, we mean a place of K which corresponds to a nonzero prime ideal of R_K. By abuse of notation, we identify any finite place v of K with its corresponding prime ideal of R_K. We denote by M_K the set of all places of K. In particular, M_K contains the finite places of K, but also the archimedean places (if K is a number field), or the places of K lying over the place at infinity from $\mathbb{F}_q(t)$ (if K is a function field); note that all but finitely many places in M_K are finite places of K.

Let $V \subset \mathbb{P}^M$ be a quasiprojective variety defined over K, let $\Phi_1, \dots, \Phi_r$ be endomorphisms of V defined over K, and let $\alpha \in V(K)$. We denote by S the monoid generated by $\Phi_1, \dots, \Phi_r$, and we let $\mathcal{O}^S(\alpha)$ be the orbit of α under the maps contained in S. Moreover we assume that for every distinct tuples $(m_1, \cdots, m_r)$ and $(n_1, \cdots, n_r)$ of nonnegative integers, we have

$$\Phi_1^{m_1} \cdots \Phi_r^{m_r}(\alpha) \neq \Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha). \tag{2.1}$$

The above condition (2.1) replaces the condition that α is not preperiodic for Φ_1 in the case $r = 1$ (see Theorem 1.1). In the case of a cyclic monoid S (i.e. $r = 1$), we need to impose the condition that α is not preperiodic for Φ_1, otherwise the orbit $\mathcal{O}^S(\alpha)$ would be finite and our problem would be vacuous. On the other hand, if (2.1) does not hold for *all* endomorphisms $\Phi_1, \dots, \Phi_r$, but it does hold for a *subset* $\Phi_1, \dots, \Phi_s$ of them, then we may replace our monoid S with the submonoid generated by $\Phi_1, \dots, \Phi_s$.

Let k_v be the residue field corresponding to any finite place v of K. Then k_v is finite; we set $\mathrm{N}(v) := \# k_v$, which we call the norm of v. We extend the notation $N(\mathfrak{a})$ to denote the size of $R_K/\mathfrak{a}$ for any nonzero ideal $\mathfrak{a}$ of R_K.

For all but finitely many finite places v of K, both V and each Φ_i for $i = 1, \dots, r$ have good reduction modulo v. In particular this means that there exists a model $\mathfrak{V}$ of V, and corresponding models for each Φ_i for $i = 1, \dots, r$ over R_K such that for all but finitely many finite places v of K, the corresponding reductions modulo v of each Φ_i induces a k_v-endomorphism of the special fibre $\mathfrak{V}_v$ of $\mathfrak{V}$ over v. Choosing different models affects only finitely many places v; therefore, from now on we assume that we fixed a model $\mathfrak{V}$ of V over R_K, and we also fixed corresponding models for Φ_i as endomorphisms of the $\mathrm{Spec}(R_K)$-scheme $\mathfrak{V}$.

There is a nonzero ideal $\mathfrak{I}_K \subset R_K$ such that if $v \nmid \mathfrak{I}_K$ then the reduction $\mathbb{P}^M(K) \to \mathbb{P}^M(k_v)$ modulo v is well defined (see [25, Lemma 9] for a proof if K is a number field; however, the same proof works also in the case of function fields using that modulo principal ideals, there are finitely many representatives for the ideal class group of R_K). More precisely, each point in $\mathbb{P}^M(K)$ has a representation as $[x_0 : \cdots : x_M]$, where each $x_i \in R_K$ and the ideal $(x_0, \dots, x_M)$ divides $\mathfrak{I}_K$. In addition, at the expense of replacing $\mathfrak{I}_K$ with a larger non-unit ideal of R_K, we may assume that for each $v \nmid \mathfrak{I}_K$, both $\mathfrak{V}$ and each Φ_i has good reduction at v. Thus, for each $v \nmid \mathfrak{I}_K$ we define $\mathcal{O}_v^S(\alpha)$ be the reduction of the S-orbit $\mathcal{O}^S(\alpha)$ of α modulo v; in particular,

$\mathcal{O}_v^S(\alpha)$ consists of all points $\Psi_v(\alpha_v) \in \mathfrak{V}_v(k_v)$ for $\Psi \in S$, where for each such $\Psi \in S$, we denote by Ψ_v its reduction modulo v to an endomorphism of $\mathfrak{V}_v$, and we also let α_v denote the reduction of α modulo v. Finally, note that each time when we refer to a place v which either divides, or it does not divide $\mathfrak{I}_K$, we implicitly assume that v is a finite place.

In order to state our main results we need to define the natural density for a set of finite places. We say that a subset $\mathcal{P}$ of finite places of K has *natural density* $\mathbf{d}\mathcal{P}$ if we have

$$\mathbf{d}\mathcal{P} := \lim_{x\to\infty} \frac{\#\{v \in \mathcal{P} :\ \mathrm{N}(v) \le x\}}{\#\{v :\ \mathrm{N}(v) \le x\}}.$$

Theorem 2.1. *With the above notation, and under the condition* (2.1)*, assume in addition that* $D := \max\{\deg(\Phi_1), \dots, \deg(\Phi_r)\} \ge 2$. *Then for each* $\epsilon < 1/(r \log D)^r$*, the set of finite places* $v \nmid \mathfrak{I}_K$ *such that* $\#\mathcal{O}_v^S(\alpha) < \epsilon\,(\log \mathrm{N}(v))^r$ *has natural density equal to* 0.

Remark 2.2. It is immediate to see that Theorem 2.1 yields that for each $\gamma < 1$, the set of finite places $v \nmid \mathfrak{I}_K$ such that $\#\mathcal{O}_v^S(\alpha) < (\log \mathrm{N}(v))^{r\gamma}$ has natural density equal to 0. To see this, note that for each $\epsilon > 0$, and for each $\gamma < 1$ there exists $C(\epsilon, \gamma) > 0$ such that for each place v satisfying $\mathrm{N}(v) > C(\epsilon, \gamma)$, we have $(\log \mathrm{N}(v))^{r\gamma} < \epsilon\,(\log \mathrm{N}(v))^r$ (also note that there are at most finitely many places v satisfying $\mathrm{N}(v) \le C(\epsilon, \gamma)$).

Theorem 2.3. *With the above notation, and under condition* (2.1)*, assume in addition that* $\deg(\Phi_i) = 1$ *for each* $i = 1, \dots, r$. *Then for each* $\gamma < r/(2r+1)$*, the set of finite places* $v \nmid \mathfrak{I}_K$ *such that* $\#\mathcal{O}_v^S(\alpha) < \mathrm{N}(v)^\gamma$ *has natural density equal to* 0.

If we assume in addition that S *is commutative, then the above result holds for* $\gamma < r/(r+1)$.

Remark 2.4. Actually, our proofs of Theorems 2.1 and 2.3 yield a stronger result: for each $x > 0$, the set of places v of K such that $\mathrm{N}(v) \le x$ for which the conclusion of either Theorem 2.1 or Theorem 2.3 does not hold has less than $\pi(x)^\alpha$ elements, for some $\alpha < 1$, where $\pi(x)$ is the number of all places v of K satisfying $\mathrm{N}(v) \le x$.

Finally, we note that in Theorem 2.3 if S is a set generated by finitely many translations on an algebraic group, we recover previous variants of the Artin's conjecture as proved in [1, 8, 16, 20].

3. Heights over global fields

We continue with the notation from Section 2.

Any global field K comes equipped with a standard set M_K of places and their associated absolute values $|\cdot|_v$ which satisfy a product formula

$$\prod_{v\in M_K} |x|_v^{n_v} = 1, \qquad \text{for every } x \in K^*,$$

where n_v is the local degree at place v (see [15] for more details). Furthermore, without loss of generality, we may assume that the normalization of the absolute values $|\cdot|_v$ and of the local degrees n_v was made such that for each nonarchimedean place v, and for each uniformizer $\pi_v \in K$ at v we have $|\pi_v|_v^{n_v} \le \frac{1}{2}$.

If K is a global field, and if $M \ge 1$, the logarithmic Weil height of $x := [x_0 : x_1 : \cdots : x_M] \in \mathbb{P}^M(K)$ (relative to K) is defined as (see [15])

$$h_K(x) = \sum_{v\in M_K} \log\left(\max_{i=0}^{M} |x_i|_v^{n_v}\right).$$

Also for $x \in K$ we set $h_K(x) = h_K([x:1])$ where $[x:1] \in \mathbb{P}^1(K)$.

In the case that K is a function field, using that each $v \in M_K$ is nonarchimedean, for any $x, y \in K$ we have

$$h_K(x+y) \le h_K(x) + h_K(y). \tag{3.1}$$

Let $x := [x_0 : x_1 : \cdots : x_M]$ and $y := [y_0 : y_1 : \cdots : y_M] \in \mathbb{P}^M(K)$ be two different points, such that each x_j and y_j is in R_K, and $(x_0, \dots, x_M, y_0, \dots, y_M) \mid \mathfrak{I}_K$. Let $\mathfrak{D} = (x_i y_j - x_j y_i)_{0 \le i < j \le M}$ be the ideal of R_K generated by elements $x_i y_j - x_j y_i$. Then, as proved in [25, Proposition 7], we have

$$\log N(\mathfrak{D}) \le h_K(x) + h_K(y) + C_0, \tag{3.2}$$

where C_0 depends only on K and M (this result is proven in [25] for number fields, but the proof follows identically for any global field).

Let $\Psi := [F_0 : \cdots : F_M]$ be any rational map on $\mathbb{P}^M$ given by $(M+1)$ relatively prime polynomials of degree $d = \deg(\Psi)$. Letting Z_Ψ be the closed subset of $\mathbb{P}^M$ where all F_i vanish simultaneously, we have the following elementary height estimate

$$h_K(\Psi(\alpha)) \le \deg(\Psi) h_K(\alpha) + C(\Psi), \tag{3.3}$$

for all $\alpha \in (\mathbb{P}^M \setminus Z_\Psi)(K)$ (see [14, Theorem B.2.5 (a)]), where $C(\Psi)$ is a positive constant depending only on Ψ. Inequality (3.3) easily extends to any endomorphism Φ of a quasiprojective subvariety $V \subset \mathbb{P}^M$ (see the definition of degree of such an endomorphism from Section 1); thus we obtain

$$h_K(\Phi(\alpha)) \le \deg(\Phi) h_K(\alpha) + C(\Phi),$$

for every $\alpha \in V(K)$. An easy inductive argument yields that if $D := \deg \Phi \ge 2$, then

$$h_K(\Phi^n(\alpha)) \le D^n (h_K(\alpha) + C(\Phi)), \text{ for each } n \in \mathbb{N}, \tag{3.4}$$

while if $\deg(\Phi) = 1$, then

$$h_K(\Phi^n(\alpha)) \le h_K(\alpha) + nC(\Phi). \tag{3.5}$$

The following two results are used in the proofs of our theorems.

Lemma 3.1. *Let K be a global field, and let R_K be its ring of integers (as defined in Section 2). Then for each nonzero ideal $\mathfrak{a}$ of R_K, the number $\omega_K(\mathfrak{a})$ of nonzero prime ideals of R_K which divide $\mathfrak{a}$ is bounded above by* $\log N(\mathfrak{a}) / \log(2)$.

Proof. Let $\mathfrak{a} = \prod_{i=1}^m \mathfrak{p}_i^{e_i}$ be the decomposition in prime ideals of $\mathfrak{a}$. Taking norms, and then applying the logarithm (note that the norm function is completely multiplicative), we obtain

$$\begin{aligned} \log N(\mathfrak{a}) &= \sum_{i=1}^m e_i \log N(\mathfrak{p}_i) \\ &\ge \log(2) \cdot \omega_K(\mathfrak{a}), \end{aligned}$$

which yields the desired conclusion. □

Lemma 3.2. *If K is a global field, then for each nonzero $x \in K$, the number $\omega_K(x)$ of finite places $v \in M_K$ such that $|x|_v < 1$ is bounded above by $h_K(x)/\log(2)$.*

Proof. Using the product formula and the definition of the logarithmic Weil height, we immediately obtain that $h_K(x) = h_K(x^{-1})$. Hence

$$\begin{aligned} h_K(x) &= h_K(x^{-1}) \\ &\geq \sum_{v \text{ is a finite place}} \log\max\{|x^{-1}|_v^{n_v}, 1\} \\ &\geq \sum_{\substack{v \text{ is a finite place} \\ |x|_v<1}} (-n_v \log|x|_v) \\ &\geq \log(2)\cdot\omega_K(x), \end{aligned}$$

where in the last inequality we used the fact that for each nonarchimedean place $v \in M_K$ such that $|x|_v < 1$, we have $|x|_v^{n_v} \leq \frac{1}{2}$. □

4. Endomorphisms of quasiprojective varieties

In this section, we have the following setting: K is a global field, $V \subset \mathbb{P}^M$ is a quasiprojective variety defined over K, and $\Phi_1, \dots, \Phi_r$ are endomorphisms of V defined over K. Let $D := \max\{\deg(\Phi_1), \dots, \deg(\Phi_r)\}$. In addition, we let $\alpha \in V(K)$ and assume that for every distinct tuples $(m_1, \dots, m_r)$ and $(n_1, \dots, n_r)$ of nonnegative integers, we have

$$\Phi_1^{m_1}\cdots\Phi_r^{m_r}(\alpha) \neq \Phi_1^{n_1}\cdots\Phi_r^{n_r}(\alpha). \tag{4.1}$$

We let S be the monoid generated by $\Phi_1, \dots, \Phi_r$, and denote by $\mathcal{O}^S(\alpha)$ the orbit of α under the action of the endomorphisms of V contained in S. We continue with the same notation for R_K, $\mathfrak{I}_K$, $\mathcal{O}_v^S(\alpha)$ (for finite places $v \nmid \mathfrak{I}_K$) as in Section 2.

We will use in our proofs the usual notation $f(x) = o(g(x))$ to denote that

$$\lim_{x\to\infty} f(x)/g(x) = 0.$$

Also we write $f(x) \sim g(x)$ if $f(x) = g(x) + o(g(x))$.

The following result is the key ingredient in the proofs of Theorems 2.1 and 2.3.

Proposition 4.1. *For each $y > 1$, let*

$$T_y := \{v \nmid \mathfrak{I}_K : \#\mathcal{O}_v^S(\alpha) < y\}.$$

(i) *If $D \geq 2$, then $\#T_y \leq C \cdot y^2 D^{ry^{\frac{1}{r}}}$, where C is a positive constant depending only on V, S and α.*
(ii) *If $D = 1$, then $\#T_y \leq C \cdot y^{2+\frac{1}{r}}$, where C is a positive constant depending only on V, S and α.*
(iii) *If $D = 1$ and S is commutative, then $\#T_y \leq C \cdot y^{1+\frac{1}{r}}$, where C is a positive constant depending only on V, S and α.*

Proof. Let $v \in T_y$; by the pigeonhole principle, there exist two distinct tuples $(m_1, \dots, m_r)$ and $(n_1, \dots, n_r)$ such that

(1) $\Phi_1^{m_1}\cdots\Phi_r^{m_r}(\alpha)$ and $\Phi_1^{n_1}\cdots\Phi_r^{n_r}(\alpha)$ have the same reduction modulo v; and
(2) $0 \leq m_i, n_i \leq [y^{1/r}]$ for each $i = 1, \dots, r$,

where $[z]$ represents the integer part of the real number z.

According to our assumption (4.1), $\Phi_1^{m_1}\cdots\Phi_r^{m_r}(\alpha)\neq\Phi_1^{n_1}\cdots\Phi_r^{n_r}(\alpha)$, which by combination with (1) means that

(1') the ideal $\mathfrak{D}:=(A_{m,i}A_{n,j}-A_{n,i}A_{m,j})_{0\le i<j\le M}$ is nonzero; and
(2') $v\mid\mathfrak{D}$,

where $\Phi_1^{m_1}\cdots\Phi_r^{m_r}(\alpha)=[A_{m,0}:\cdots:A_{m,M}]$ and $\Phi_1^{n_1}\cdots\Phi_r^{n_r}(\alpha)=[A_{n,0}:\cdots:A_{n,M}]$, while each $A_{m,j}$ and $A_{n,j}$ is in R_K, and $(A_{m,0},\dots,A_{m,M},A_{n,0},\dots,A_{n,M})\mid\mathfrak{I}_K$.

(i) Assume $D\ge 2$. By employing (3.2) and (3.4), we have

$$\begin{aligned}\log N(\mathfrak{D}) &\le h_K(\Phi_1^{m_1}\cdots\Phi_r^{m_r}(\alpha))+h_K(\Phi_1^{n_1}\cdots\Phi_r^{n_r}(\alpha))+C_1\\ &\le C_2\cdot D^{ry^{\frac{1}{r}}},\end{aligned}$$

where the constants C_1 and C_2 depend only on $\Phi_1,\dots,\Phi_r$ and α. Using (2') and Lemma 3.1 and noting that there are at most $\left([y^{\frac{1}{r}}]+1\right)^{2r}\le 2^{2r}y^2$ pairs of tuples $(m_1,\dots,m_r)$ and $(n_1,\dots,n_r)$ satisfying (2) above, we obtain the desired conclusion.

(ii) Assume $D=1$. By employing (3.2) and (3.5), we have

$$\begin{aligned}\log N(\mathfrak{D}) &\le h_K(\Phi_1^{m_1}\cdots\Phi_r^{m_r}(\alpha))+h_K(\Phi_1^{n_1}\cdots\Phi_r^{n_r}(\alpha))+C_1\\ &\le C_2\cdot y^{\frac{1}{r}},\end{aligned}\tag{4.2}$$

where the constants C_1 and C_2 depend only on r, $\Phi_1,\dots,\Phi_r$ and α. Using Lemma 3.1 and noting that there are at most 4^ry^2 pairs of tuples $(m_1,\dots,m_r)$ and $(n_1,\dots,n_r)$ satisfying (2) above, we obtain the desired conclusion.

(iii) Now, if S is commutative (still assuming $D=1$), then we may refine our application of the pigeonhole principle. Indeed, besides (1) and (2) above, we may also consider

(3) for each $i=1,\dots,r$, either $m_i=[y^{1/r}]$ or $n_i=[y^{1/r}]$.

We may add condition (3) to the previously stated conditions (1) and (2) because for each tuples $(m_1,\dots,m_r)$ and $(n_1,\dots,n_r)$ satisfying conditions (1) and (2), and for each $i=1,\dots,r$ we obtain that also

$$\Phi_i^{[y^{1/r}]-\max\{m_i,n_i\}}\left(\Phi_1^{m_1}\cdots\Phi_r^{m_r}(\alpha)\right)\ \text{and}\ \Phi_i^{[y^{1/r}]-\max\{m_i,n_i\}}\left(\Phi_1^{n_1}\cdots\Phi_r^{n_r}(\alpha)\right)$$

have the same reduction modulo v (here we also use the fact that Φ_i has good reduction modulo $v\nmid\mathfrak{I}_K$). There are at most $2^r\cdot\left([y^{1/r}]+1\right)^r\le 4^ry$ pairs of tuples $(m_1,\dots,m_r)$ and $(n_1,\dots,n_r)$ satisfying conditions (2) and (3). This observation together with (4.2) will finish the proof. ☐

Using Proposition 4.1 we obtain immediately Theorems 2.1 and 2.3. We prove below Theorem 2.1; the proof of Theorem 2.3 is similar.

Proof of Theorem 2.1. Let $\epsilon<1/(r\log D)^r$. We prove first the number field case and then the function field case.

(i) If K is a number field, let

$$R_{\epsilon,x}:=\{v\nmid\mathfrak{I}_K:\ \mathrm{N}(v)\le x\ \text{and}\ \#\mathcal{O}_v^S(\alpha)<\epsilon\,(\log\mathrm{N}(v))^r\}.$$

So by Proposition 4.1

$$\begin{aligned} \# R_{\epsilon,x} &\leq \# T_{\epsilon(\log x)^r} \\ &\leq C\left(\epsilon(\log x)^r\right)^2 D^{r(\epsilon(\log x)^r)^{\frac{1}{r}}} \\ &= C\epsilon^2(\log x)^{2r}\cdot x^{r\log(D)\epsilon^{\frac{1}{r}}} \\ &= o\left(x/\log x\right), \end{aligned}$$

because $\epsilon < 1/(r\log D)^r$. Note that in a number field, the number of places v with $\mathrm{N}(v) \leq x$ is asymptotic to $x/\log x$, which finishes our proof.

(ii) If K is a function field with constant field $\mathbb{F}_q$, we have

$$\#\{v \in M_K : \ \mathrm{N}(v) \leq q^\ell\} \sim \frac{q}{q-1}\cdot\frac{q^\ell}{\ell},$$

as $\ell \to \infty$, where ℓ is a variable taking values in positive integers (see [22, Theorem 5.12]).

Let

$$R_{\epsilon,q^\ell} := \{v \nmid \mathfrak{I}_K : \ \mathrm{N}(v) \leq q^\ell \text{ and } \#\mathcal{O}_v^S(\alpha) < \epsilon\left(\log \mathrm{N}(v)\right)^r\}.$$

So, similar to part (i), by Proposition 4.1 we have

$$\# R_{\epsilon,q^\ell} \leq \# T_{\epsilon(\log q^\ell)^r} = o\left(\frac{q^\ell}{\ell}\right),$$

if $\epsilon < 1/(r\log D)^r$. Therefore

$$\# R_{\epsilon,q^\ell} = o\left(\frac{q}{q-1}\cdot\frac{q^\ell}{\ell}\right)$$

as desired. $\square$

5. The case of Drinfeld modules

We begin by defining a Drinfeld module (for more details, see [7, 12, 22]). Let p be a prime and let q be a power of p. Let K be a function field with constant field $\mathbb{F}_q$, and let $\overline{K}$ be a fixed algebraic closure of K. We let τ be the Frobenius on $\mathbb{F}_p$, and we extend its action on $\overline{K}$ (i.e., $\tau(x) = x^p$ for each $x \in \overline{K}$). The ring $\mathrm{End}(\mathbb{G}_a/K)$ of endomorphisms of the additive group scheme over K is isomorphic to the skewed ring $K\{\tau\}$ of polynomials in the operator τ with coefficients in K; more precisely, each $f \in \mathrm{End}(\mathbb{G}_a/K)$ is of the form $\sum_{i=0}^r a_i\tau^i$ with $a_i \in K$, and $f(x) = \sum_{i=0}^r a_i x^{p^i}$ for each $x \in \overline{K}$.

Let $A := \mathbb{F}_p[t]$. A Drinfeld module is a ring homomorphism

$$\begin{array}{rccc} \rho & : & A & \rightarrow & K\{\tau\} \\ & & f(t) & \mapsto & \rho_{f(t)} \end{array} \text{ such that } \rho_t := t\tau^0 + a_1\tau^1 + \cdots + a_n\tau^n,$$

with $a_i \in K$, and $a_n \neq 0$ where $n \geq 1$. We call n the rank of the Drinfeld module ρ.

For every field extension $K \subset L$, the Drinfeld module ρ induces an action of $\mathbb{F}_p[t]$ on $\mathbb{G}_a(L)$ by $f(t) * x := \rho_{f(t)}(x)$, for each $f(t) \in \mathbb{F}_p[t]$. We call $\mathbb{F}_p[t]$-*submodules* subgroups of $\mathbb{G}_a(\overline{K})$ which are invariant under the action of ρ. Because from now on we will work with a fixed Drinfeld module ρ, we simply call $\mathbb{F}_p[t]$-submodule any $\mathbb{F}_p[t]$-submodule Γ under the action of ρ. We define the *rank* of such an $\mathbb{F}_p[t]$-submodule Γ be $\dim_{\mathbb{F}_p(t)} \Gamma \otimes_{\mathbb{F}_p[t]} \mathbb{F}_p(t)$.

We note that usually, in the definition of a Drinfeld module, A is the ring of functions defined on a projective nonsingular curve C defined over a finite field $\mathbb{F}_{p^m}$ (for some $m \geq 1$), regular away from a closed point $\eta \in C$. For our definition of a Drinfeld module, $C = \mathbb{P}^1_{\mathbb{F}_p}$ and η is the usual point at infinity on $\mathbb{P}^1$. On the other hand, every ring of regular functions A as above contains $\mathbb{F}_p[t]$ as a subring, where t is a nonconstant function in A. So, in particular, any A-submodule is also an $\mathbb{F}_p[t]$-submodule; therefore, our results for $\mathbb{F}_p[t]$-submodules (see Theorem 5.2) can be used to infer results about arbitrary A-submodules under the action of any Drinfeld module.

A point $\alpha \in \overline{K}$ is *torsion* for the Drinfeld module action if and only if there exists $f(t) \in \mathbb{F}_p[t] \setminus \{0\}$ such that $\rho_{f(t)}(\alpha) = 0$. In other words, α is a torsion point if and only if it generates a finite cyclic $\mathbb{F}_p[t]$-submodule.

For each finite place v of K such that the coefficients of ρ_t are v-adic integers, we reduce each $\rho_{f(t)}$ modulo v (it is immediate to see that for each $f(t) \in \mathbb{F}_p[t]$, also each coefficient of $\rho_{f(t)}$ is a v-adic integer); we denote by $S_{\rho,K}$ the set of all these finite places v of K.

Let r be a positive integer, and let $\Gamma \subset K$ be a free $\mathbb{F}_p[t]$-submodule of rank r (according to [21], the field K is the direct sum of a finite torsion $\mathbb{F}_p[t]$-submodule with a free $\mathbb{F}_p[t]$-submodule of rank $\aleph_0$). There are only finitely many places $v \in S_{\rho,K}$ such that the elements of Γ are not integral at v. Indeed, if $x_1, \dots, x_r \in K$ is a fixed set of generators for the free $\mathbb{F}_p[t]$-submodule Γ, then each element of Γ is integral at places $v \in S_{\rho,K}$ whenever each x_i is integral at v. For each such finite place v, we denote by Γ_v the corresponding reduction of Γ. We let $S_{\Gamma,\rho,K}$ be the set of all such finite places of K for which there exists a corresponding reduction Γ_v of Γ; note that $S_{\Gamma,\rho,K}$ contains all but finitely many places of K.

The following result is the counterpart for Drinfeld modules of Proposition 4.1.

Proposition 5.1. *For each positive integer $\ell \geq 1$, let*

$$\tilde{T}_\ell := \{v \in S_{\Gamma,\rho,K} : \#\Gamma_v \leq q^\ell\}.$$

There exists a constant C depending only on ρ, Γ and K such that

$$\#\tilde{T}_\ell \leq C \cdot q^{\ell(1+n/r)}.$$

Proof. First we let e be a positive integer such that $q = p^e$.

Let $v \in \tilde{T}_\ell$; then a simple application of the pigeonhole principle yields that there exist polynomials $f_1(t), \dots, f_r(t) \in \mathbb{F}_p[t]$, not all zero, such that

(i) $|\sum_{i=1}^r \rho_{f_i(t)}(x_i)|_v < 1$, and
(ii) $\deg(f_i(t)) \leq (e\ell)/r$, for each $i = 1, \dots, r$.

According to Lemma 3.2 (also note that $\sum_{i=1}^r \rho_{f_i(t)}(x_i) \neq 0$ because Γ is a free $\mathbb{F}_p[t]$-module and not all $f_i(t)$ are zero), the number of places v satisfying (i) is bounded above by

$$\frac{1}{\log(2)} \cdot h_K\left(\sum_{i=1}^r \rho_{f_i(t)}(x_i)\right).$$

We rewrite $\sum_{i=1}^r \rho_{f_i(t)}(x_i)$ as $\sum_{j=0}^m \rho_{t^j}(y_j)$, for some positive integer $m \leq (e\ell)/r$, where each y_j is an $\mathbb{F}_p$-linear combination of the x_i's; thus there are finitely many possibilities for the y_j's. Now, using (ii), the triangle inequality for heights (3.1), and inequality (3.4) applied to ρ_t (which has degree p^n), we obtain that

$$\frac{1}{\log(2)} \cdot h_K\left(\sum_{i=1}^{r} \rho_{f_i(t)}(x_i)\right) \leq C_1 p^{ne\ell/r},$$

where C_1 depends only on ρ and $x_1, \ldots, x_r$. We conclude that $\#\tilde{T}_\ell$ is bounded above by

$$\sum_{\deg(a_1),\ldots,\deg(a_r)\leq(e\ell)/r} C_1 \cdot p^{ne\ell/r} \leq C_2 \cdot q^{\ell(1+n/r)},$$

as desired. □

Now we are ready to prove our main result for Drinfeld modules, which is part (i) of Theorem 1.4.

Theorem 5.2. *With the above notation for K, ρ and Γ, let $\gamma < r/(r+n)$. Then the natural density of the set of places $v \in S_{\Gamma,\rho,K}$ such that $\#\Gamma_v < \mathrm{N}(v)^\gamma$ equals* 0.

Proof. Let

$$\tilde{R}_{\gamma,\ell} = \left\{ v \in S_{\Gamma,\rho,K} :\ \mathrm{N}(v) \leq q^\ell \text{ and } \#\Gamma_v < (\mathrm{N}(v))^\gamma \right\}.$$

Observe that

$$\#\tilde{R}_{\gamma,\ell} \quad\leq\quad \#\tilde{T}_{\gamma\ell}$$

where $\tilde{T}_{\gamma\ell}$ is defined in Proposition 5.1. Now an application of Proposition 5.1 yields

$$\#\tilde{R}_{\gamma,\ell} \leq \#\tilde{T}_{\gamma\ell} \leq C \cdot q^{\gamma\ell(1+n/r)},$$

where C depends on ρ, Γ, and K. Since $\gamma < r/(r+n)$, we conclude that

$$\#\tilde{R}_{\gamma,\ell} = o\left(\frac{q}{q-1} \cdot \frac{q^\ell}{\ell}\right),$$

as desired. □

Part (ii) of Theorem 1.4 follows similarly. For example, in the case of a trivial $\mathbb{F}_p[t]$-action on the function field K given by $t * x := tx$, the result of Proposition 5.1 changes to

$$\#\tilde{T}_\ell \leq C_\epsilon \cdot q^{\ell(1+\epsilon)}, \tag{5.1}$$

for any $\epsilon > 0$, where C_ϵ is a constant depending only on ϵ, ρ, Γ and K. Indeed, now the action of $\mathbb{F}_p[t]$ on K is given by linear maps, and thus the height of $f(t) * x$ grows linearly with respect to $\deg(f(t))$. Using (5.1) one immediately obtains the conclusion of part (ii) in Theorem 1.4 for any nontrivial $\mathbb{F}_p[t]$-submodules (the case of $\mathbb{Z}$-modules under the trivial action of $\mathbb{Z}$ given by $k * x := kx$ follows similarly).

References

[1] A. Akbary and K. Murty, *Reduction mod p of subgroups of the Mordell-Weil group of an elliptic curve*, Int. J. Number Theory, to appear, 27 pages.

[2] M. H. Baker and R. Rumely, *Equidistribution of small points, rational dynamics, and potential theory*, Ann. Inst. Fourier (Grenoble) **56** (2006), 625–688.

[3] J. P. Bell, D. Ghioca, and T. J. Tucker, *A dynamical Mordell-Lang problem for étale maps*, submitted for publication (2008), available at `http://arxiv.org/abs/0808.3266`, 19 pages.

[4] R. L. Benedetto, D. Ghioca, P. Kurlberg, and T. J. Tucker, *A dynamical Mordell-Lang theorem for curves*, submitted for publication (2008), available at `http://arxiv.org/abs/0712.2344`, 18 pages.

[5] G. S. Call and J. H. Silverman, *Canonical heights on varieties with morphisms*, Compositio Math. **89** (1993), 163–205.

[6] A. Chambert-Loir, *Mesures et équidistribution sur les espaces de Berkovich*, J. Reine Angew. Math. **595** (2006), 215–235.

[7] L. Denis, *Hauteurs canoniques et modules de Drinfeld*, Math. Ann. **294** (1992), no. 2, 213–223.

[8] P. Erdös and R. Murty, *On the order of a (mod p)*, CRM Proceedings and Lecture Notes, Volume **19**, 1999, 87–97.

[9] C. Favre and J. Rivera-Letelier, *Équidistribution quantitative des points de petite hauteur sur la droite projective*, Math. Ann. **335** (2006), 311–361.

[10] D. Ghioca and T. J. Tucker, *Proof of a dynamical Bogomolov conjecture for lines under polynomial actions*, submitted for publication (2008), available at `http://arxiv.org/abs/0808.3263`, 5 pages.

[11] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math. **171** (2008), 463–483.

[12] D. Goss, *Basic structures of function field arithmetic*, Springer-Verlag, New York, 1998.

[13] R. Gupta and R. Murty, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), 13–44.

[14] M. Hindry and J. H. Silverman, *Diophantine geometry. An introduction*, Graduate Texts in Mathematics, **201**, Springer-Verlag, New York, 2000.

[15] S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983.

[16] C. R. Matthews, *Counting points modulo p for some finitely generated subgroups of algebraic groups*, Bull. London Math. Soc. **14** (1982), 149–154.

[17] P. Morton and J. H. Silverman, *Rational periodic points of rational functions*, Internat. Math. Res. Notices **2** (1994), 97–110.

[18] P. Morton and J. H. Silverman, *Periodic points, multiplicities, and dynamical units*, J. Reine Angew. Math. **461** (1995), 81–122.

[19] D. G. Northcott, *Periodic points on an algebraic variety*, Ann. of Math. (2) **51** (1950), 167–177.

[20] F. Pappalardi, *On the order of finitely generated subgroups of* $\mathbb{Q}^*$ *(mod p) and divisors of* $p-1$, J. Number Theory **57** (1996), 207–222.

[21] B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfeld modules*, Compositio Math. **97** (1995), no. 3, 349–368.

[22] M. Rosen, *Number Theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York, 2002.

[23] J. H. Silverman, *Rational points on* $K3$ *surfaces: a new canonical height*, Invent. Math. **105** (1991), 347–373.

[24] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, **241**, Springer-Verlag, New-York, 2007.

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

[26] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, **46**, Cambridge University Press, 1995.

[27] S. Zhang, *Distributions in algebraic dynamics*, Surveys in differential geometry, **10**, 381–430, International Press, 2006.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada
E-mail address: amir.akbary@uleth.ca

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada
E-mail address: dragos.ghioca@uleth.ca