THE DYNAMICAL MORDELL-LANG CONJECTURE FOR ENDOMORPHISMS OF SEMIABELIAN VARIETIES DEFINED OVER FIELDS OF POSITIVE CHARACTERISTIC

P. CORVAJA, D. GHIOCA, T. SCANLON, AND U. ZANNIER

Abstract. Let K be an algebraically closed field of prime characteristic p, let X be a semiabelian variety defined over a finite subfield of K, let $\Phi : X \longrightarrow X$ be a regular self-map defined over K, let $V \subset X$ be a subvariety defined over K, and let $\alpha \in X(K)$. The Dynamical Mordell-Lang Conjecture in characteristic p predicts that the set $S = \{n \in \mathbb{N} \colon \Phi^n(\alpha) \in V\}$ is a union of finitely many arithmetic progressions, along with finitely many p-sets, which are sets of the form $\left\{\sum_{i=1}^m c_i p^{k_i n_i} \colon n_i \in \mathbb{N}\right\}$ for some $m \in \mathbb{N}$, some rational numbers c_i and some non-negative integers k_i. We prove that this conjecture is equivalent with some difficult diophantine problem in characteristic 0. In the case X is an algebraic torus, we can prove the conjecture in two cases: either when $\dim(V) \leq 2$, or when no iterate of Φ is a group endomorphism which induces the action of a power of the Frobenius on a positive dimensional algebraic subgroup of X.

1. Introduction

In this paper, as a matter of convention, any subvariety of a given variety is assumed to be closed. We denote by $\mathbb{N}$ the set of positive integers, we let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, and let p be a prime number. An arithmetic progression is a set of the form $\{mk + \ell : \ k \in \mathbb{N}_0\}$ for some $m, \ell \in \mathbb{N}_0$; note that when $m = 0$, this set is a singleton. For a set X endowed with a self-map Φ, and for $m \in \mathbb{N}_0$, we let Φ^m denote the m-th iterate $\Phi \circ \cdots \circ \Phi$, where Φ^0 denotes the identity map on X. If $\alpha \in X$, we define its orbit under Φ as $\mathcal{O}_\Phi(\alpha) := \{\Phi^n(\alpha) \colon n \in \mathbb{N}_0\}$.

Motivated by the classical Mordell-Lang conjecture proved by Faltings [Fal94] (for abelian varieties) and Vojta [Voj96] (for semiabelian varieties), the Dynamical Mordell-Lang Conjecture predicts that for a quasiprojective

2010 *Mathematics Subject Classification.* Primary: 11G10, Secondary: 37P55.

Key words and phrases. Dynamical Mordell-Lang problem, endomorphisms of semiabelian varieties defined over fields of characteristic p.

The second author has been partially supported by a Discovery Grant from the National Science and Engineering Board of Canada. The third author has been partially supported by grant DMS-1363372 of the United States National Science Foundation and a Simons Foundation Fellowship.

variety X endowed with a (regular) self-map Φ defined over a field K of characteristic 0, given a point $\alpha \in X(K)$ and a subvariety V of X, the set

$$S := \{n \in \mathbb{N}_0 \colon \Phi^n(\alpha) \in V(K)\}$$

is a finite union of arithmetic progressions (see [GT09, Conjecture 1.7] and also, for a thorough discussion of the Dynamical Mordell-Lang Conjecture, see the book [BGT16]).

With the above notation for X, Φ, K, V, α, S, if K has characteristic p then S may be infinite without containing an infinite arithmetic progression (see [BGT16, Example 3.4.5.1] and [Ghi, Example 1.2]). Similar to the classical Mordell-Lang conjecture in characteristic p, one has to take into account varieties defined over finite fields (see the proof of the classical Mordell-Lang conjecture in positive characteristic by Hrushovski [Hru96]). So, motivated by the structure theorem of Moosa-Scanlon [MS04] describing in terms of F-sets the intersection of a subvariety of a semiabelian variety (defined over a finite field) with a finitely generated group (see also [Ghi08]), the following conjecture was advanced.

Conjecture 1.1 (Dynamical Mordell-Lang Conjecture in positive characteristic)**.** *Let X be a quasiprojective variety defined over a field K of characteristic p. Let $\alpha \in X(K)$, let $V \subseteq X$ be a subvariety defined over K, and let $\Phi : X \longrightarrow X$ be an endomorphism defined over K. Then the set $S := S(X, \Phi, V, \alpha)$ consisting of all $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V(K)$ is a union of finitely many arithmetic progressions along with finitely many sets of the form*

$$\left\{ \sum_{j=1}^{m} c_j p^{k_j n_j} \ : \ n_j \in \mathbb{N}_0 \text{ for each } j = 1, \dots m \right\}, \tag{1}$$

for some $m \in \mathbb{N}$, some $c_j \in \mathbb{Q}$, and some $k_j \in \mathbb{N}_0$.

A set as in (1) is called a *p-set*.

Now, clearly, the set S may contain infinite arithmetic progressions if V contains some periodic subvariety under the action of Φ which intersects $\mathcal{O}_\Phi(\alpha)$. As an aside, we note that if X is a semiabelian variety (see Section 2.1) and Φ is a group endomorphism of X, then the periodic subvarieties of $V \subset X$ under the action of Φ are necessarily translates of subgroups contained in V; such translates can be classified and the maximal subgroups corresponding to them are finite in number (for more details, see [BG06, Zan09]). On the other hand, it is possible for S to contain nontrivial sets of the form (1) (where m may be larger than 1 and also where the c_i's may not be integers, as shown by [Ghi, Examples 1.2 and 1.4]). It is likely that all cases when the set of solutions S is infinite, but it is not a finite union of arithmetic progressions occur in the presence of an algebraic group; however, proving this assertion is probably just as difficult as the original Conjecture 1.1.

So far, Conjecture 1.1 is known to hold in the following two cases:

(i) if X is a semiabelian variety defined over a finite field and Φ is an algebraic group endomorphism whose action on the tangent space at the identity is given through a diagonalizable matrix (see [BGT16, Proposition 13.3.0.2]). Actually, [BGT16, Proposition 13.3.0.2] was stated only in the special case $X = \mathbb{G}_m^N$, but the proof carries over almost verbatim for the general case of semiabelian varieties defined over a finite field. Furthermore, in this case, the set S from the conclusion of Conjecture 1.1 consists only of finitely many arithmetic progressions, i.e., the more complicated p-sets from (1) do not appear.

(ii) if $X = \mathbb{G}_m^N$ and $V \subset X$ is a curve (see [Ghi, Theorem 1.3]). In this case, the p-sets from (1) may appear, but they consist of only one nontrivial power of the prime p (i.e., $m \leq 2$ and $k_1 = 0$ with the notation as in (1)).

In this paper we prove two new results towards Conjecture 1.1 by showing it holds for any surface contained in $\mathbb{G}_m^N$ and for any regular self-map $\Phi : \mathbb{G}_m^N \longrightarrow \mathbb{G}_m^N$ (not necessarily a group endomorphism), and also prove that it holds for any subvariety $V \subset \mathbb{G}_m^N$ assuming Φ is an algebraic group endomorphism with the property that no iterate of it restricts to being a power of the Frobenius on a proper algebraic subgroup of $\mathbb{G}_m^N$.

Theorem 1.2. *Let $\Phi : \mathbb{G}_m^N \longrightarrow \mathbb{G}_m^N$ be a regular self-map defined over an algebraically closed field K of characteristic p, let $V \subset \mathbb{G}_m^N$ be a variety of dimension at most equal to 2, and let $\alpha \in \mathbb{G}_m^N(K)$. Then the set of $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V(K)$ is a finite union of arithmetic progressions along with finitely many sets of the form*

$$\left\{c_0 + c_1 p^{k_1 n_1} + c_2 p^{k_2 n_2} : n_1, n_2 \in \mathbb{N}_0\right\}, \tag{2}$$

for some $c_0, c_1, c_2 \in \mathbb{Q}$ and some $k_1, k_2 \in \mathbb{N}_0$.

We remark that Theorem 1.2 in the case V is a surface formally implies the conclusion of Theorem 1.2 in the case of curves; hence, it suffices to assume V is an irreducible surface in the hypotheses of Theorem 1.2.

As shown in [Ghi, Example 1.2] (which provides the example of a hypersurface $V \subset \mathbb{G}_m^3$), there are examples of surfaces $V \subset \mathbb{G}_m^N$ whose intersection with an orbit of a regular self-map of $\mathbb{G}_m^N$ yields a set as in (2) where c_1, c_2, k_1, k_2 are all nonzero.

Theorem 1.3. *Let $\Phi : \mathbb{G}_m^N \longrightarrow \mathbb{G}_m^N$ be an algebraic group endomorphism, let $V \subset \mathbb{G}_m^N$ be a subvariety defined over an algebraically closed field of characteristic p, and let $\alpha \in \mathbb{G}_m^N(K)$. Assume there is no nontrivial connected algebraic subgroup G of $\mathbb{G}_m^N$ such that an iterate of Φ induces an endomorphism of G, which equals a power of the usual Frobenius. Then the set of $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V(K)$ is a finite union of arithmetic progressions*

along with finitely many sets of the form

$$\left\{ \sum_{j=1}^{m} c_j p^{k_j n_j} \ : \ n_j \in \mathbb{N}_0 \text{ for each } j = 1, \dots m \right\},$$

for some $m \in \mathbb{N}$, *some* $c_j \in \mathbb{Q}$, *and some* $k_j \in \mathbb{N}_0$.

Both Theorems 1.2 and 1.3 are proved by showing that in these cases, Conjecture 1.1 reduces to some questions regarding polynomial-exponential equations, which can be solved with the known Diophantine tools. More generally, we prove that Conjecture 1.1 in the more general case of an arbitrary group endomorphism of $\mathbb{G}_m^N$ reduces to some deep Diophantine questions, whose solution is well-beyond the presently known techniques.

Theorem 1.4. *Let* $\{u_k\}$ *be a linear recurrence sequence of integers, let* $m, c_1, \dots, c_m \in \mathbb{N}$, *and let* p *be a prime number with* $\sum_{i=1}^{m} c_i < p - 1$. *Then there exists* $N \in \mathbb{N}$, *there exists an algebraically closed field* K, *there exists an algebraic group endomorphism* $\Phi : \mathbb{G}_m^N \longrightarrow \mathbb{G}_m^N$, *there exists* $\alpha \in \mathbb{G}_m^N(K)$ *and there exists a subvariety* $V \subset \mathbb{G}_m^N(K)$ *such that the set of all* $n \in \mathbb{N}_0$ *for which* $\Phi^n(\alpha) \in V(K)$ *is precisely the set of all* $n \in \mathbb{N}_0$ *such that*

$$u_n = \sum_{i=1}^{m} c_i p^{n_i}, \tag{3}$$

for some $n_1, \dots, n_m \in \mathbb{N}_0$.

The polynomial-exponential equation (3) is very deep and despite an extensive research being done on this problem, the case of a general linear recurrence sequence $\{u_n\}$ coupled with $m > 2$ (i.e., at least three powers of the prime p in (3)) is beyond the known methods (for more details, see [CZ00, CZ13]). We also note that applying a similar construction as in the proof of Theorem 1.4, one can establish a similar result in the context of arbitrary semiabelian varieties X defined over a finite field; in this case, the right hand-side of (3) is replaced by some linear combination of powers of the roots of the minimal polynomial in $\mathbb{Z}[x]$ which kills the Frobenius acting on X (in the case $X = \mathbb{G}_m^N$, the minimal polynomial in $\mathbb{Z}[x]$ killing the Frobenius is simply $x - p$; for more details, see Section 2.1, especially equation (4)).

Finally, we note that since already the case of semiabelian varieties is very difficult, it is hard to predict how one can approach Conjecture 1.1 for other ambient quasiprojective varieties X; also, many of the p-adic tools used in proving special cases of the Dynamical Mordell-Lang Conjecture in characteristic 0 (see [BGT16, Chapter 6]) do not work in positive characteristic.

We discuss now the strategy for proving our results. We have two main ingredients for the proof of Theorems 1.2 and 1.3: on one hand, we have Theorem 2.2 (see also the more precise statement from Corollary 2.4 in the case of intersections with surfaces), and on the other hand, we have various Diophantine results regarding solutions to polynomials-exponential equations

(see Theorem 5.1). With the notation as in Theorems 1.2 and 1.3, there exists a finitely generated group Γ such that the orbit of α under Φ is contained inside Γ, and so, we obtain $V(K)\cap\mathcal{O}_\Phi(\alpha)$ by intersecting first V with Γ and then with $\mathcal{O}_\Phi(\alpha)$. As we will prove in Theorem 3.2 (see also Theorem 1.4 for the converse statement), solving Conjecture 1.1 for regular self-maps on $\mathbb{G}_m^N$ reduces to solving polynomial-exponential equations of the form (3). If V is a surface, we use Corollary 2.4 to reduce to the case there are at most 2 powers of p in the right-hand side from (3); this allows us to completely solve the case of surfaces contained in a torus. Similarly, the hypothesis from Theorem 1.3 on the endomorphism Φ of $\mathbb{G}_m^N$ reduces the polynomial-exponential equation from (3) to a Diophantine question, which we know how to answer. Apart from these two cases, the polynomial-exponential equations of type (3) are beyond the reach of the known Diophantine methods.

We sketch below the plan of our paper. In Section 2.2 we discuss the classical Mordell-Lang problem for semiabelian varieties in characteristic p, by stating the results of Moosa-Scanlon [MS04] and then explaining their connections to Conjecture 1.1 (we also note the papers [Der07, DM12], which treat related problems). In Section 2.3 we also discuss some properties of the p-sets, i.e., sets of the form (1). Then we proceed in Section 3 to prove that Conjecture 1.1 for regular self-maps of semiabelian varieties X defined over a finite field reduces to a polynomial-exponential question (see Theorem 3.2). We stress out that our result applies to *all* semiabelian varieties X; in particular, this would allow future researchers to use Theorem 3.2 for solving additional cases of Conjecture 1.1 for semiabelian varieties X once there will be new progress to solving the polynomial-exponential equations corresponding to Conjecture 1.1. In Section 4, we prove that in the case $X=\mathbb{G}_m^N$, then we actually recover a *large class* of possible polynomial-exponential equations (this is Theorem 1.4); so, the results from Section 4 may be viewed as complementary to the results from Section 3. In Section 5, we establish the key Diophantine statement for our proofs of Theorems 1.2 and 1.3. We conclude our paper by proving Theorems 1.2 and 1.3 in Section 6.

2. The Mordell-Lang problem in positive characteristic

2.1. **Semiabelian varieties.** From now on, p is a prime number, K is an algebraically closed field of characteristic p, and X is a semiabelian variety defined over K, i.e., there exists a short exact sequence of algebraic groups defined over K:

$$1\longrightarrow T\longrightarrow X\longrightarrow A\longrightarrow 1,$$

where A is an abelian variety and T is an algebraic torus (possibly trivial). Each regular self-map Φ of X is a composition of a translation with an (algebraic group) endomorphism Φ_0. Indeed, after composing Φ with a translation, we may assume Φ sends the identity of X into itself. In particular, this means that the induced map $\varphi:=\Phi|_T$ is a regular self-map on the torus T, which maps the identity into itself; hence φ is an endomorphism

of T. Furthermore, the induced map $\bar{\Phi} : A \longrightarrow A$ also maps the identity into itself and so, it must be a group endomorphism as well (see [Mil, Corollary 1.2]). Since there is no non-constant regular map between an abelian variety and a torus, we derive that Φ must be a group endomorphism, as claimed.

Each endomorphism $\Phi_0 : X \longrightarrow X$ is integral over $\mathbb{Z}$ (where $\mathbb{Z}$ is seen as a subring of the ring $\mathrm{End}(X)$ of endomorphisms of X), i.e., there exists $\ell \in \mathbb{N}$ and there exist integers $c_0, \ldots, c_{\ell-1}$ such that

$$\Phi_0^\ell + c_{\ell-1}\Phi_0^{\ell-1} + \cdots + c_1\Phi_0 + c_0 \cdot \mathrm{Id} = 0, \tag{4}$$

where the above identity endomorphism Id is seen inside $\mathrm{End}(X)$. Actually, $\ell \leq 2\dim(X)$, but this fact will not be necessary in our proof.

Assume X is defined over a finite subfield $\mathbb{F}_q$ of K, and let F be the corresponding Frobenius map for the finite field $\mathbb{F}_q$; we extend F to an endomorphism of X. Then also F satisfies an equation of the form (4); furthermore, as a consequence of Weil conjectures for abelian varieties over finite fields, we note that the roots of the corresponding minimal equation satisfied by the endomorphism F are distinct and each one has absolute value equal to q^{a_i} with $a_i \in \left\{\frac{1}{2}, 1\right\}$. Actually, we know more precise information about the rational numbers a_i (i.e., there is at most one $a_i = 1$ and if some $a_i = 1$ then the corresponding root of (4) equals q and the torus T is nontrivial, while there are $2\cdot\dim(A)$ roots of absolute value $q^{\frac{1}{2}}$, according to Weil conjectures [Mil, Chapter 2]); however, the only relevant information for us will be that the roots for the minimal equation satisfied by F are distinct and their absolute values are of the form q^{a_i} for some positive $a_i \in \mathbb{Q}$.

2.2. **The intersection of a subvariety of a semiabelian variety defined over a finite field with a finitely generated subgroup.** We continue with the notation from Section 2.1 for K and X. We assume X is defined over a finite subfield $\mathbb{F}_q \subset K$, and we let V be an arbitrary subvariety of X defined over K. In order to state Theorem 2.2 (which is crucial for all our proofs), we need first to introduce the notion of *F-sets* defined by Moosa-Scanlon [MS04]. The Frobenius F acting on X is the endomorphism induced by the usual field homomorphism given by $x \mapsto x^q$ for each $x \in K$.

Definition 2.1. *With the above notation for X, q, K and F, let $\Gamma \subseteq X(K)$ be a finitely generated subgroup.*

(a) *By a* sum of F-orbits *in Γ we mean a set of the form*

$$C(\alpha_1, \ldots, \alpha_m; k_1, \ldots, k_m) := \left\{ \sum_{j=1}^{m} F^{k_j n_j}(\alpha_j) \colon n_j \in \mathbb{N}_0 \right\} \subseteq \Gamma$$

where $\alpha_1, \ldots, \alpha_m$ are some given points in $X(K)$ and $k_1, \ldots, k_m$ are some given non-negative integers.

(b) *An* F-set *in* Γ *is a set of the form* $C + \Gamma'$ *where* C *is a sum of* F-*orbits in* Γ*, and* $\Gamma' \subseteq \Gamma$ *is a subgroup, while in general, for two sets* $A, B \subset X(K)$*, then* $A + B$ *is simply the set* $\{a + b\colon a \in A,\ b \in B\}$.

As a matter of convention, when we work with F-orbits inside an algebraic torus $\mathbb{G}_m^N$ (corresponding to the usual Frobenius map $x \mapsto x^p$), then we call *product* of F-orbits, rather than sum of F-orbits; also, in this case we use the notation $\prod_{j=1}^m \alpha_j^{p^{k_j n_j}}$ for an element in the corresponding product of F-orbits (as in part (a) of Definition 2.1).

We note that allowing for the possibility that some $k_i = 0$ in the definition of a sum of F-orbits, implicitly we allow a singleton be a sum of F-orbits; this also explains why we do not need to consider cosets of subgroups Γ' in the definition of an F-set. Furthermore, if $k_2 = \cdots = k_m = 0$ then the corresponding sum of F-orbits is simply a translate of the single F-orbit $C(\alpha_1; k_1)$. Note that the F-orbit $C(\alpha; k)$ for $k > 0$ is finite if and only if $\alpha \in X\left(\overline{\mathbb{F}_p}\right)$. Finally, we call an orbit $C(\alpha; k)$ nontrivial, if it is infinite (i.e., $k > 0$ and $\alpha \notin X\left(\overline{\mathbb{F}_p}\right)$).

We also note that since we allow the base points a_i be outside Γ, we can use the slightly simpler definition of groupless F-sets involving sums of F-orbits rather than using the F-cycles (see [MS04, Remark 2.6], and also the slight extension proven in [Ghi08]).

Theorem 2.2 (Moosa-Scanlon [MS04])**.** *Let* X *be a semiabelian variety defined over* $\mathbb{F}_q$*, let* $\mathbb{F}_q \subset K$ *be an algebraically closed field, let* $V \subset X$ *be a subvariety defined over* K *and let* $\Gamma \subset X(K)$ *be a finitely generated subgroup. Then* $V(K) \cap \Gamma$ *is a finite union of* F*-sets contained in* Γ.

Remark 2.3. One can deduce following the argument from [MS04] that each sum of F-orbits appearing in the interrsection of V with the group Γ is a sum of at most $\dim(V)$ nontrivial orbits; this follows easily from the proof of [MS04, Theorem 7.8] using induction on the dimension of V (see also [MS04, Corollary 7.3]). Also, in the case X is an algebraic torus, Derksen-Masser [DM12, Theorem 1] (see also the paper by Masser [Mas04] on a similar topic) proved that there are at most $\dim(V)$ nontrivial orbits under the Frobenius in any product of F-orbits appearing in the intersection of $V \subset \mathbb{G}_m^N$ with Γ.

We state below a special case of these results which we will employ in our proof of Theorem 1.2; the next corollary can be deduced also directly using a similar argument as in the proof of [Ghi, Corollary 2.3].

Corollary 2.4. *With the notation from Theorem 2.2, if* $X = \mathbb{G}_m^N$ *and* V *is a surface, then the intersection* $V(K) \cap \Gamma$ *is a finite union of* F*-sets* $C \cdot \Gamma'$*, where* C *is a product of orbits under the Frobenius action on* $\mathbb{G}_m^N$ *of which at most* 2 *orbits are nontrivial, while* Γ' *is a subgroup of* Γ.

2.3. **Arithmetic sequences.** In this section (which overlaps with [Ghi, Section 3]) we state various useful results regarding linear recurrence sequences and p-sets.

A *linear recurrence sequence* is a sequence $\{u_n\}_{n\in\mathbb{N}_0} \subset \mathbb{C}$ with the property that there exists $m \in \mathbb{N}$ and there exist $c_0, \dots, c_{m-1} \in \mathbb{C}$ such that for each $n \in \mathbb{N}_0$ we have

$$u_{n+m} + c_{m-1}u_{n+m-1} + \cdots + c_1 u_{n+1} + c_0 u_n = 0. \tag{5}$$

If $c_0 = 0$ in (5), then we may replace m by $m-k$ where k is the smallest positive integer such that $c_k \neq 0$; then the sequence $\{u_n\}_{n\in\mathbb{N}_0}$ satisfies the linear recurrence relation

$$u_{n+m-k} + c_{m-1}u_{n+m-1-k} + \cdots + c_k u_n = 0, \tag{6}$$

for all $n \geq k$. In particular, if $k = m$, then the sequence $\{u_n\}_{n\in\mathbb{N}_0}$ is eventually constant, i.e., $u_n = 0$ for all $n \geq m$.

Assume now that $c_0 \neq 0$ (which may be achieved at the expense of re-writing the recurrence relation as in (6)); then there exists a closed form for expressing u_n for all n (or at least for all n sufficiently large if one needs to re-write the recurrence relation as in (6)). The characteristic roots of a linear recurrence sequence as in (5) are the solutions of the equation

$$x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0 = 0. \tag{7}$$

We let r_i (for $1 \leq i \leq s$) be the (nonzero) roots of the equation (7); then there exist polynomials $P_i(x) \in \mathbb{C}[x]$ such that for all $n \in \mathbb{N}_0$, we have

$$u_n = \sum_{i=1}^{s} P_i(n) r_i^n. \tag{8}$$

In general, as explained above, for an arbitrary linear recurrence sequence, the formula (8) holds for all n sufficiently large (more precisely, for all $n \geq m$ with the notation from (5)); for more details on linear recurrence sequences, we refer the reader to the chapter on linear recurrence sequences written by Schmidt [Sch03].

It will be convenient for us later on in our proof to consider linear recurrence sequences which are given by a formula such as the one in (8) (for n sufficiently large) for which the following two properties hold:

(i) if some r_i is a root of unity, then $r_i = 1$; and
(ii) if $i \neq j$, then r_i/r_j is not a root of unity.

Such linear recurrence sequences given by formula (8) and satisfying properties (i)-(ii) above are called *non-degenerate*. Given an arbitrary linear recurrence sequence, we can always split it into finitely many linear recurrence sequences which are all non-degenerate; moreover, we can achieve this by considering instead of one sequence $\{u_n\}$, finitely many sequences which are all of the form $\{u_{nM+\ell}\}$ for a given $M \in \mathbb{N}$ and for $\ell = 0, \dots, M-1$. Indeed, assume some r_i or some r_i/r_j is a root of unity, say of order M; then for each $\ell = 0, \dots, M-1$ we have that

$$u_{nM+\ell} = \sum_{i=1}^{s} P_i(nM+\ell) r_i^{\ell} (r_i^M)^n \tag{9}$$

and moreover, we can re-write the formula (9) for $u_{nM+\ell}$ by collecting the powers r_i^M which are equal and thus achieve a non-degenerate linear recurrence sequence $v_n := u_{nM+\ell}$.

The following famous theorem of Skolem [Sko34] (later generalized by Mahler [Mah56] and Lech [Lec53]) will be used throughout our proof.

Proposition 2.5. *Let $\{u_n\}_{n\in\mathbb{N}_0} \subset \mathbb{C}$ be a linear recurrence sequence, and let $c \in \mathbb{C}$. Then the set T of all $n \in \mathbb{N}_0$ such that $u_n = c$ is a finite union of arithmetic progressions; moreover, if $\{u_n\}$ is a non-degenerate linear recurrence sequence, then the set T is infinite only if the sequence $\{u_n\}$ is eventually constant.*

Next we consider the p-sets, which are sets of non-negative integers of the form (1), i.e.,

$$\left\{ \sum_{j=1}^{m} c_j p^{k_j n_j} : n_j \in \mathbb{N}_0 \right\} \tag{10}$$

for some $m \in \mathbb{N}$, some $c_j \in \mathbb{Q}$ and some $k_j \in \mathbb{N}_0$. Since for each positive integer M, the powers of p are preperiodic modulo M, we immediately obtain the following result.

Proposition 2.6. *Let p be a prime number. The intersection of an arithmetic progression with a p-set is a finite union of p-sets.*

Also, as a simple application of Laurent's theorem [Lau84] regarding the intersection of subvarieties of an algebraic torus T with finitely generated subgroups of T, we obtain the following result.

Proposition 2.7. *The intersection of two p-sets is a finite union of p-sets. More precisely, if each of the two p-sets that we intersect consists of sums of at most m powers of p (see (10)), then each p-set from their intersection also consists of sums of at most m powers of p as in (10).*

3. Reduction of the dynamical problem to a polynomial-exponential equation

Our goal is to prove that solving Conjecture 1.1 reduces to solving several polynomial-exponential equations (see Theorem 3.2). In order to state our result, we introduce some notation.

In this section, we fix some finite field $\mathbb{F}_q$ of characteristic p; also, we let X be a semiabelian variety defined over $\mathbb{F}_q$. We let F be the Frobenius endomorphism of X induced by the field automorphism $x \mapsto x^q$. We let $P_{\min,F} \in \mathbb{Z}[x]$ be the minimal polynomial for the Frobenius (as an endomorphism of X); then $P_{\min,F}$ has simple roots: $\lambda_1, \dots, \lambda_r$. So,

$$P_{\min,F} \text{ is a monic polynomial of degree } r \text{ and } P_{\min,F}(F) = 0. \tag{11}$$

Let $\{U_n\}_{n\in\mathbb{N}_0}$ be a linear recurrence sequence. Let $m \in \mathbb{N}_0$, let $\{U_n^{(i)}\}_{n\in\mathbb{N}_0} \subset \mathbb{Z}$ (for $i = 1, \dots, m$) be linear recurrence sequences, each one of them having

simple characteristic roots, all of them being of the form $\lambda_j^{b_i}$ for some $b_i \in \mathbb{N}_0$ (where the λ_j's are the minimal roots of the minimal polynomial $P_{\min,F} \in \mathbb{Z}[x]$ of the Frobenius endomorphism of X). In particular, if $b_i = 0$ then $U^{(i)}$ is a constant sequence because it is a linear recurrence sequence which has only one characteristic root, which is equal to 1. So, if $U^{(i)}$ is a constant sequence (i.e., if $b_i = 0$), then we say that $U^{(i)}$ is a trivial sequence, while if $U^{(i)}$ is non-constant (i.e., if $b_i \in \mathbb{N}$), then we say that $U^{(i)}$ is a nontrivial sequence.

Then, with the above notation for the linear recurrence sequences U and $U^{(i)}$, given also some $a, b \in \mathbb{N}_0$, we call an *F-arithmetic sequence*, the set of all n of the form $ak+b$ (for some $k \in \mathbb{N}_0$) for which there exist $n_1, \dots, n_m \in \mathbb{N}_0$ such that

$$U_n = U^{(1)}_{n_1} + \cdots + U^{(m)}_{n_m}. \tag{12}$$

Remarks 3.1. The following observations will be used repeatedly in the proof of Theorem 3.2.

(i) If $m = 0$, then Equation 12 is void and in this case, the F-arithmetic sequence is simply the arithmetic progression $\{ak + b\}_{k\in\mathbb{N}_0}$.

(ii) On the other hand, if $a = 0$ (regardless of $m \in \mathbb{N}_0$), then the corresponding F-arithmetic sequence contains at most one element $\{b\}$.

(iii) In general, we could combine the two conditions defining the F-arithmetic sequence into one condition:

$$U_{ak+b} = U^{(1)}_{n_1} + \cdots + U^{(m)}_{n_m}. \tag{13}$$

However, we prefer to work with Equation 12 instead and tacitly assume that the set of solutions n must also belong to an arithmetic progression. Note that the sequence $\{U_{ak+b}\}_{k\in\mathbb{N}_0}$ is itself a linear recurrence sequence whose characteristic roots are the a-th powers of the characteristic roots of the linear recurrence sequence U.

The intersection of finitely many F-arithmetic sequences is called a *general F-arithmetic sequence*.

Theorem 3.2. *With the above notation for p, q, X and F, let $\Phi : X \longrightarrow X$ be a regular self-map defined over an algebraically closed field K containing $\mathbb{F}_q$, let $\alpha \in X(K)$ and let $V \subset X$ be a subvariety defined over K. Then the set of all $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V(K)$ is a union of finitely many general F-arithmetic sequences.*

Furthermore, the following more precise statements hold:

(1) *The number of nontrivial linear recurrence sequences $U^{(i)}$ appearing in the definition of each F-arithmetic sequence from the conclusion of Theorem 3.2 (see (12)) is at most equal to* $\dim(V)$.

(2) *If Φ is a group endomorphism, then the characteristic roots of the linear recurrence sequences $\{U_n\}$ appearing in the left-hand side of each equation (12) defining any of the above general F-arithmetic*

sequences are positive integer powers of the roots of the minimal polynomial in $\mathbb{Z}[x]$ satisfied by Φ (see equation (4)).

Remark 3.3. Since a (generalized) F-arithmetic sequence may be a singleton (see Remark 3.1 (ii)), our conclusion in Theorem 3.2 allows for finite sets to appear as the return set of $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V(K)$. Similarly, as noted in Remark 3.1 (i), we also allow the possibility of an arithmetic progression to appear as the return set in Theorem 3.2.

Remark 3.4. Because we want to establish the more precise statement (2) from the conclusion of Theorem 3.2, we prefer to use Equation 12 rather than Equation 13 when working with an F-arithmetic sequence (see also Remark 3.1 (iii)).

Proof of Theorem 3.2. Since X is a semiabelian variety, then there exists a group endomorphism $\Phi_0 : X \longrightarrow X$ and there exists $y \in X(K)$ such that for any $\gamma \in X$, we have that $\Phi(\gamma) = \Phi_0(\gamma) + y$. Also, as noted in (4), there exists $\ell \in \mathbb{N}$ such that Φ_0 satisfies (in $\mathrm{End}(X)$) a monic equation of degree ℓ with integer coefficients. Then, as shown in [Ghi, Claim 4.2] (whose proof for algebraic tori extends verbatim for any semiabelian variety), there exist linear recurrence sequences $\{u_n^{(i)}\}_{n\in\mathbb{N}_0} \subset \mathbb{Z}$ for $1 \leq i \leq \ell$ and $\{v_n^{(i)}\}_{n\in\mathbb{N}_0} \subset \mathbb{Z}$ for $0 \leq i \leq \ell - 1$ such that for each $n \in \mathbb{N}_0$, we have

$$\Phi^n(\alpha) = \sum_{i=1}^{\ell} u_n^{(i)} \left(\sum_{j=0}^{i-1} \Phi_0^j(y) \right) + \sum_{i=0}^{\ell-1} v_n^{(i)} \Phi_0^i(\alpha). \tag{14}$$

Furthermore, the characteristic roots of the linear recurrence sequences $v^{(i)}$ are among the roots of the minimal polynomial $P_{\min,\Phi_0} \in \mathbb{Z}[x]$ of Φ_0, while the characteristic roots of $u^{(i)}$ are contained in the set consisting of 1 and all of the roots of $P_{\min,\Phi_0}$ (see [Ghi, Equations (14) and (17)]).

We also use the following notation

$$Q_i := \sum_{j=0}^{i-1} \Phi_0^j(y) \text{ for each } i = 1, \ldots, \ell. \tag{15}$$

We let Γ be a finitely generated group containing $\Phi_0^j(y)$ and $\Phi_0^j(\alpha)$ for each $j = 0, \ldots, \ell - 1$. Theorem 2.2 yields that

$$V(K) \cap \Gamma \text{ is a finite union of } F\text{-sets } C + H \text{ contained in } \Gamma, \tag{16}$$

where C is a sum of F-orbits (actually, we have at most $\dim(V)$ nontrivial orbits appearing in C, as observed in Remark 2.3—see also Corollary 2.4) and H is a subgroup of Γ. Thus we write

$$C = \left\{ \sum_{j=1}^{m} F^{n_j k_j}(\gamma_j) \colon n_j \in \mathbb{N}_0 \right\}, \tag{17}$$

for some $m \in \mathbb{N}_0$, some $\gamma_j \in X(K)$ and some $k_j \in \mathbb{N}_0$, and moreover, there are at most $\dim(V)$ nonzero k_i's.

At the expense of replacing Γ by a larger (but still finitely generated) group, we may assume Γ contains each $F^i(\gamma_j)$ for $j = 1, \dots, m$ and $i = 0, \dots, r-1$. In particular, we get that $F^i(\gamma_j) \in \Gamma$ for all $i \geq 0$ (see (11)).

Since Γ is a finitely generated abelian group, we know that it is isomorphic to a direct sum of a finite subgroup Γ_0 with a subgroup Γ_1 which is isomorphic to $\mathbb{Z}^s$ for some $s \in \mathbb{N}_0$. We let $\{P_1, \dots, P_s\}$ be a $\mathbb{Z}$-basis for Γ_1.

We proceed with the notation from equations (14) and (15) and so,

$$\Phi^n(\alpha) = \sum_{i=1}^{\ell} u_n^{(i)} Q_i + \sum_{i=0}^{\ell-1} v_n^{(i)} \Phi_0^i(\alpha).$$

Then we write each Q_i (for $i = 1, \dots, \ell$) as $Q_{i,0} + \sum_{j=1}^{s} b_{i,j} P_j$ with $Q_{i,0} \in \Gamma_0$ and each $b_{i,j} \in \mathbb{Z}$, and also write each $\Phi_0^i(\alpha)$ (for $i = 0, \dots, \ell-1$) as $T_{i,0} + \sum_{j=1}^{s} c_{i,j} P_j$ with $T_{i,0} \in \Gamma_0$ and each $c_{i,j} \in \mathbb{Z}$.

We also write for each $j = 1, \dots, m$ and for each $i = 0, \dots, r-1$ (note that r is the degree of the minimal polynomial $P_{\min,F}$ with integer coefficients satisfied by the Frobenius endomorphism in $\mathrm{End}(X)$; see equation (11))

$$F^i(\gamma_j) = R_{j,0}^{(i)} + \sum_{k=1}^{s} d_{i,j,k} P_k \text{ with } R_{j,0}^{(i)} \in \Gamma_0 \text{ and each } d_{i,j,k} \in \mathbb{Z}.$$

We will write the conditions satisfied by $n \in \mathbb{N}_0$ in order for $\Phi^n(\alpha) \in (C+H)$ (see (16)), or equivalently that there exist some $n_1, \dots, n_m \in \mathbb{N}_0$ such that

$$\Phi^n(\alpha) - \sum_{j=1}^{m} F^{k_j n_j}(\gamma_j) \in H.$$

In order to do this, we observe that, similar to deducing the formula (14), we have that there exist linear recurrence sequences $\{a_n^{(i)}\}_{n \in \mathbb{N}_0} \subset \mathbb{Z}$ for $i = 0, \dots, r-1$ such that

$$F^n(\gamma_j) = \sum_{i=0}^{r-1} a_n^{(i)} F^i(\gamma_j). \tag{18}$$

Furthermore, for each $i = 0, \dots, r-1$, the characteristic equation satisfied by the linear recurrence sequence $\{a_n^{(i)}\}_{n \in \mathbb{N}_0}$ is $P_{\min,F}(x) = 0$. Indeed, this follows from the fact that $P_{\min,F}(F) = 0$ and then expressing reccursively F^n as linear combinations of F^i (for $i = 0, \dots, r-1$) with integer coefficients $a_n^{(i)}$ and then observing that each sequence $\{a_n^{(i)}\}_{n \in \mathbb{N}_0}$ satisfies the linear recurrence given by the characteristic equation $P_{\min,F}(x) = 0$.

We compute then

$$\begin{aligned}
&\Phi^n(\alpha) - \sum_{i=1}^{m} F^{k_i n_i}(\gamma_i) \\
= &\left(\sum_{i=1}^{\ell} u_n^{(i)} Q_{i,0} + \sum_{i=0}^{\ell-1} v_n^{(i)} T_{i,0} - \sum_{j=0}^{r-1} \sum_{i=1}^{m} a_{k_i n_i}^{(j)} R_{i,0}^{(j)} \right) \\
+ &\sum_{k=1}^{s} \left(\sum_{i=1}^{\ell} b_{i,k} u_n^{(i)} + \sum_{i=0}^{\ell-1} c_{i,k} v_n^{(i)} - \sum_{j=0}^{r-1} \sum_{i=1}^{m} d_{j,i,k} a_{k_i n_i}^{(j)} \right) \cdot P_k.
\end{aligned}$$

Since linear combinations of linear recurrence sequences are again linear recurrence sequences (whose characteristic roots are among the characteristic roots of the original linear recurrence sequences), we conclude that there exist linear recurrence sequences $\{U_n^{(k)}\}_{n\in\mathbb{N}_0}$ for $k = 1, \ldots, s$ and $\{A_n^{(i,k)}\}_{n\in\mathbb{N}_0}$ for $i = 1, \ldots, m$ and $k = 1, \ldots, s$ such that

$$\begin{aligned}
&\Phi^n(\alpha) - \sum_{i=1}^{m} F^{k_i n_i}(\gamma_j) \\
= &\left(\sum_{i=1}^{\ell} u_n^{(i)} Q_{i,0} + \sum_{i=0}^{\ell-1} v_n^{(i)} T_{i,0} - \sum_{j=0}^{r-1} \sum_{i=1}^{m} a_{k_i n_i}^{(j)} R_{i,0}^{(j)} \right) \\
+ &\sum_{k=1}^{s} \left(U_n^{(k)} - \sum_{i=1}^{m} A_{n_i}^{(i,k)} \right) P_k.
\end{aligned}$$

More precisely, $U_n^{(k)} := \sum_{i=1}^{\ell} b_{i,k} u_n^{(i)} + \sum_{i=0}^{\ell-1} c_{i,k} v_n^{(i)}$. In particular, if $\Phi = \Phi_0$ (i.e., if $y = 0$) then $U_n^{(k)} = \sum_{i=0}^{\ell-1} c_{i,k} v_n^{(i)}$ and so, the characteristic roots of each $U^{(k)}$ is among the characteristic roots of the $v^{(i)}$'s, i.e., the characteristic roots of the $U^{(k)}$'s are among the roots of $P_{\min,\Phi}$. Also, for each $i = 1, \ldots, m$, each $k = 1, \ldots, s$ and for each $n \in \mathbb{N}_0$, we have that

$$A_n^{(i,k)} := \sum_{j=0}^{r-1} d_{j,i,k} a_{k_i n}^{(j)}.$$

In particular, if $k_i = 0$ (i.e., the corresponding F-orbit $C(\gamma_i; k_i)$ is trivial), then $A^{(i,k)}$ is a trivial linear recurrence sequence (i.e., it is constant). Furthermore, the characteristic roots for each linear recurrence sequence $A^{(i,k)}$ are k_i-th powers of the eigenvalues λ_j of the Frobenius F.

Now, since each $Q_{i,0}$, $T_{i,0}$ and $R_{i,0}^{(j)}$ is a torsion point (of order bounded by the cardinality M of the torsion subgroup of Γ) and moreover, any linear recurrence sequence of integers is preperiodic modulo M, then at the expense of replacing each n and also each n_i by suitable arithmetic progressions (which, in particular, leads to replacing $U^{(k)}$ and $A^{(i,k)}$ by other linear

recurrence sequences whose characteristic roots are powers of the characteristic roots for the original linear recurrence sequences), we may assume there exists some torsion point $S_0 \in \Gamma$ such that

$$\begin{aligned} & \Phi^n(\alpha) - \sum_{j=1}^{m} F^{k_j n_j}(\gamma_j) \\ = \quad & S_0 + \sum_{k=1}^{s} \left(U_n^{(k)} - \sum_{i=1}^{m} A_{n_i}^{(i,k)} \right) P_k. \end{aligned}$$

Replacing n by an arithmetic progression $\{an+b\}_{n\in\mathbb{N}_0}$ (for some $a \in \mathbb{N}$ and $b \in \mathbb{N}_0$) simply changes Φ by Φ^a and also replaces α by $\Phi^b(\alpha)$. Also, the conclusion of Theorem 3.2 is unaffected by this change since for any linear recurrence sequence $\{w_n\}_{n\in\mathbb{N}_0}$, the sequence $\{w_{an+b}\}_{n\in\mathbb{N}_0}$ satisfies also a linear recurrence and its characteristic roots are the a-th powers of the characteristic roots of $\{w_n\}_{n\in\mathbb{N}_0}$; see also Remark 3.1 (iii).

So, we need to determine for which $n \in \mathbb{N}_0$ there exist some $n_1, \dots, n_m \in \mathbb{N}_0$ such that $\Phi^n(\alpha) - \sum_{j=1}^{m} F^{k_j n_j}(\gamma_j) \in H$, or equivalently, for which $n \in \mathbb{N}_0$ we have that

$$\sum_{k=1}^{s} \left(U_n^{(k)} - \sum_{i=1}^{m} A_{n_i}^{(i,k)} \right) P_k \in -S_0 + H. \tag{19}$$

Now, according to [Ghi08, Claim 3.4, Definition 3.5, Subclaim 3.6], the condition (19) is equivalent with a system formed by finitely many equations either of the form

$$\sum_{k=1}^{s} e_k \cdot \left(U_n^{(k)} - \sum_{i=1}^{m} A_{n_i}^{(i,k)} \right) = 0, \tag{20}$$

for some integers e_k, or of the form

$$\sum_{k=1}^{s} f_k \cdot \left(U_n^{(k)} - \sum_{i=1}^{m} A_{n_i}^{(i,k)} \right) \equiv 0 \pmod{L} \tag{21}$$

for some integers f_k and some $L \in \mathbb{N}$. The solutions $(n, n_1, \cdots, n_m)$ to each congruence equation (21) is a finite union of sets of the form

$$\{(an+b, a_1 n_1 + b, \cdots, a_m n + b_m) \colon n, n_1, \cdots, n_m \in \mathbb{N}_0\}$$

for some $a, a_i, b, b_i \in \mathbb{N}_0$ (for $i = 1, \dots, m$). Therefore, again refining our analysis to finitely many arithmetic progressions, we may reduce to the case that n (along with $n_1, \dots, n_m$) satisfies finitely many equations of the form (20).

Each equation of the form (20) reduces to

$$W_n = \sum_{i=1}^{m} B_{n_i}^{(i)}, \tag{22}$$

where $W_n := \sum_{k=1}^{s} e_k U_n^{(k)}$ and $B_n^{(i)} := \sum_{k=1}^{s} e_k \cdot A_n^{(i,k)}$. So, $\{W_n\}_{n\in\mathbb{N}_0}$ is another linear recurrence sequence, while $\{B_n^{(i)}\}_{n\in\mathbb{N}_0}$ are linear recurrence sequences whose characteristic roots are the same as the characteristic roots of the original sequences $A^{(i,k)}$. In particular, the characteristic roots of $B^{(i)}$ are of the form $\lambda_j^{b_i}$ for some $b_i \in \mathbb{N}_0$, where the λ_j's are the roots of $P_{\min,F}$; note that $b_i = 0$ if some $k_i = 0$ and so, there are at most $\dim(V)$ nontrivial linear recurrence sequences $B^{(i)}$ as we vary $i = 1, \ldots, m$. Furthermore, the characteristic roots of the linear recurrence sequence $\{W_n\}$ are positive integer powers of the roots of $P_{\min,\Phi_0}$ and perhaps, also equal to 1 if Φ is not a group endomorphism (i.e., $y \neq 0$); on the other hand, if $\Phi = \Phi_0$ (i.e., $y = 0$), then the characteristic roots of W are all positive integer powers of the roots of $P_{\min,\Phi} = P_{\min,\Phi_0}$. Finally, we note that if $m = 0$ then Equation 22 is void and therefore, the corresponding F-arithmetic sequence is simply an arithmetic progression; see Remark 3.1 (i).

This concludes our proof of Theorem 3.2. □

4. Recovering a large class of polynomial-exponential equations as part of proving Conjecture 1.1

In this section we use a coding trick from [SY14] to show that not only does the dynamical Mordell-Lang problem reduce to solving polynomial-exponential equations, but conversely complicated polynomial-exponential equations may be realized as instances of the dynamical Mordell-Lang problem.

We start by extracting a key fact from [SY14].

Proposition 4.1. *Let $\{u_n\}$ be a linear recurrence sequence of integers, G a commutative algebraic group over some field K and $P \in G(K)$ a K-rational point on G. Then there are a natural number $N \in \mathbb{N}$, morphisms of algebraic groups $\Phi : G^N \to G^N$ and $\pi : G^N \to G$, and a point $Q \in G^N(K)$ so that for every $n \in \mathbb{N}_0$ we have $\pi(\Phi^n(Q)) = [u_n]_G(P)$.*

Proof. By Proposition 4.3 and Theorem 4.5 of [SY14] there are a natural number $N \in \mathbb{N}$, a vector $a \in \mathbb{Z}^N$, and linear maps $\phi : \mathbb{Z}^N \to \mathbb{Z}^N$ and $\varpi : \mathbb{Z}^N \to \mathbb{Z}$ so that for every natural number $n \in \mathbb{N}_0$ we have $\varpi(\phi^n(a)) = u_n$. Write a as $a = (a_1, \ldots, a_N)$ and ϕ and ϖ as matrices, so that $\phi(x_1, \ldots, x_N) = (\sum_{j=1}^{N} \phi_{1,j}x_j, \ldots, \sum_{j=1}^{N} \phi_{N,j}x_j)$ and $\varpi(x_1, \ldots, x_N) = \sum_{j=1}^{N} \varphi_j x_j$. Set $Q := ([a_1]_G(P), \ldots, [a_N]_G(P))$, where $a := (a_1, \ldots, a_N)$, let $\Phi : G^N \to G^N$ be the map $(x_1, \ldots, x_N) \mapsto (\sum_{j=1}^{N}[\phi_{1,j}]_G(x_j), \ldots, \sum_{j=1}^{N}[\phi_{N,j}]_G(x_j))$ and let $\pi : G^N \to G$ be the map $(x_1, \ldots, x_N) \mapsto \sum_{j=1}^{N}[\varpi_j]_G(x_j)$. Then for $n \in \mathbb{N}$ we have $\pi(\Phi^n(Q)) = [u_n]_G(P)$. □

It follows from Proposition 4.1 that we can realize many sets defined by conditions of the form $u_n \in E$ where $\{u_n\}$ is a linear recurrence sequence of integers and $E \subseteq \mathbb{N}$ is a p-set as dynamical return sets. More precisely, we have the following proposition.

Proposition 4.2. *Let $\{u_n\}$ be a linear recurrence sequence of integers, G a commutative algebraic group over the field K, $X \subseteq G$ a subvariety, $P \in G(K)$ a K-rational point on G, and $E := \{n \in \mathbb{Z} : [n]_G(P) \in X(K)\}$. Then there is an algebraic dynamical system (Y, Φ) over K, a point $Q \in Y(K)$ and a subvariety $Z \subseteq Y$ so that for all $n \in \mathbb{N}_0$ one has $\Phi^n(Q) \in Z(K) \iff u_n \in E$.*

Proof. Let N, Φ, π and Q be given by Proposition 4.1 applied to $\{u_n\}$, G, and P. Set $Y := G^N$ and $Z := \pi^{-1}(X)$; this yields the conclusion of Proposition 4.2. □

Many p-sets are known to be realizable as the exponent sets for instances of the Mordell-Lang problem in characteristic p. With the next proposition, which is inspired by special examples constructed in [Nel17], we note that it is true in particular for sets of the form $\{\sum_{i=1}^{\ell} c_i p^{n_i} : (n_1, \dots, n_\ell) \in \mathbb{N}_0^\ell\}$ with $c_1, \dots, c_\ell \in \mathbb{N}$ provided that $\sum_{i=1}^{\ell} c_i < p - 1$.

Proposition 4.3. *Let $\ell \in \mathbb{N}$, $c_1, \dots, c_\ell \in \mathbb{N}$ and $p \in \mathbb{N}$ be a prime number satisfying $\sum_{i=1}^{\ell} c_i < p - 1$. Then there is an algebraic torus G over $\mathbb{F}_p$, a subvariety $X \subseteq G$ over $\mathbb{F}_p$ and a point $P \in G(\mathbb{F}_p(t))$ so that if $E := \{m \in \mathbb{Z} : [m]_G(P) \in X(\mathbb{F}_p(t))\}$, then $E = \{\sum_{j=1}^{\ell} c_j p^{n_j} : (n_1, \dots, n_m) \in \mathbb{N}_0^\ell\}$.*

Proof. We begin with the case of $c_1 = c_2 = \cdots = c_\ell = 1$ and then use this result to deduce the general result.

The Vandermonde matrix

$$\left(a^j\right)_{\substack{1 \le a \le p-1 \\ 0 \le j < p-1}},$$

regarded as a $(p-1) \times (p-1)$ matrix over $\mathbb{F}_p$, is invertible. Write its inverse as

$$\left(A_{j,a}\right)_{\substack{1 \le a \le p-1 \\ 0 \le j < p-1}}$$

so that for $0 \le k < p-1$ and $j \in \mathbb{Z}$ we have

$$\sum_{a \in \mathbb{F}_p^\times} A_{k,a} a^j = \begin{cases} 1 & \text{if } j \equiv k \pmod{p-1} \\ 0 & \text{otherwise.} \end{cases} \tag{23}$$

Let $G := \mathbb{G}_m^{p-1}$. Set $P := (t+1, t+2, \dots, t+p-1) \in G(\mathbb{F}_p(t))$. Let $X \subseteq G$ be the subvariety defined by the equations

$$\sum_{i=1}^{p-1} A_{\ell,i} x_i = 1 \text{ and } \sum_{i=1}^{p-1} A_{k,i} x_i = 0 \text{ for } \ell < k \le p-1.$$

It is easy to see that X is the variety parametrized by the map

$$\pi : (y_1, \dots, y_\ell) \mapsto \left(\prod_{j=1}^{\ell} (y_j + 1), \prod_{j=1}^{\ell} (y_j + 2), \dots, \prod_{j=1}^{\ell} (y_j + p - 1) \right). \tag{24}$$

In particular, if $n_1, \dots, n_\ell \in \mathbb{N}_0$ and $m = \sum_{i=1}^{\ell} p^{n_i}$, then

$$\begin{aligned}
[m]_G(P) &= ((t+1)^m, \dots, (t+p-1)^m) \\
&= \left((t+1)^{\sum_{i=1}^{\ell} p^{n_i}}, \dots, (t+p-1)^{\sum_{i=1}^{\ell} p^{n_i}}\right) \\
&= \left(\prod_{i=1}^{\ell}(t+1)^{p^{n_i}}, \dots, \prod_{i=1}^{\ell}(t+p-1)^{p^{n_i}}\right) \\
&= \left(\prod_{i=1}^{\ell}(t^{p^{n_i}}+1), \dots, \prod_{i=1}^{\ell}(t^{p^{n_i}}+p-1)\right) \in X(\mathbb{F}_p(t)).
\end{aligned}$$

Let us now show that if $[m](P) \in X(\mathbb{F}_p(t))$, then m is a sum of ℓ powers of p. Considering poles of $(t+i)^m$ (for $i = 1, \dots, p-1$), one sees that if $m < 0$, then $[m](P) \notin X(\mathbb{F}_p(t))$. Indeed, taking $b \in \mathbb{F}_p^\times$ for which $A_{\ell,b} \neq 0$, we see that if $m < 0$, then the order of the pole at $-b$ of $\sum_{a \in \mathbb{F}_p^\times} A_{\ell,a}(t+a)^m$ is $-m$; so, in particular, this sum is not equal to 1.

Take now $m \geq 0$. Expanding, we have

$$\begin{aligned}
1 &= \sum_{a \in \mathbb{F}_p^\times} A_{\ell,a}(t+a)^m \\
&= \sum_{a \in \mathbb{F}_p^\times} A_{\ell,a} \sum_{j=0}^{m} \binom{m}{j} a^j t^{m-j} \\
&= \sum_{j=0}^{m} t^{m-j} \binom{m}{j} \sum_{a \in \mathbb{F}_p^\times} A_{\ell,a} a^j
\end{aligned}$$

Equating the coefficients of the powers of t, we see that

$$1 = \sum_{a \in \mathbb{F}_p^\times} A_{\ell,a} a^m \tag{25}$$

and that for $j < m$ we have

$$0 = \binom{m}{j} \sum_{a \in \mathbb{F}_p^\times} A_{\ell,a} a^j \ . \tag{26}$$

In particular, Equation 25 implies that

$$m \equiv \ell \pmod{p-1}. \tag{27}$$

Let us write m in its base p expansion, so that

$$m = \sum_i m(i,p) p^i \text{ with } 0 \leq m(i,p) < p.$$

Then $m \equiv \sum_i m(i,p) \pmod{p-1}$ and therefore, congruence equation (27) yields that

$$\sum_i m(i,p) \geq \ell. \tag{28}$$

Therefore, in order to obtain the desired conclusion in this special case of Proposition 4.3 (when $c_1 = \cdots = c_\ell = 1$), it suffices to prove that $\sum_i m(i,p) \leq \ell$.

Now, assuming we have a strict inequality in (28), then we can find some positive integer j having a base p expansion strictly dominated by that of m, that is, if we write

$$j = \sum_i j(i,p)p^i \text{ with } 0 \leq j(i,p) < p,$$

then for all i we have $j(i,p) \leq m(i,p)$ but $j(i,p) < m(i,p)$ for some i, and moreover, we can choose j so that $j \equiv \ell \pmod{p-1}$.

As Gauß observed (see [Eis95, Lemma 15.21]), $\binom{m}{j} \not\equiv 0 \pmod{p}$. Thus, from Equation 26, we see that $\sum_{a \in \mathbb{F}_p^\times} A_{\ell,a} a^j = 0$, but as $j \equiv \ell$, this contradicts Equation 23. Hence, $\sum m(i,p) \leq \ell$, which combined with inequality (28), yields that m must be the sum of exactly ℓ powers of p.

For the general case (i.e., arbitrary c_i satisfying the inequality $\sum_{i=1}^{\ell} c_i < p-1$), we first adjust the notation somewhat taking $\ell' := \sum_i c_i$ and let $X' \subseteq \mathbb{G}_{\mathrm{m}}^{p-1}$ be the variety constructed above corresponding to $\ell' < p-1$. Let $X \subseteq X'$ be the subvariety parametrized by the map

$$\nu : (y_1, \ldots, y_\ell) \mapsto \left(\prod_{j=1}^{\ell} (y_j+1)^{c_j}, \prod_{j=1}^{\ell} (y_j+2)^{c_j}, \ldots, \prod_{j=1}^{\ell} (y_j+p-1)^{c_j} \right)$$

which may be seen as the composite of π with a multidiagonal map from $\mathbb{A}^\ell$ to $\mathbb{A}^{\ell'}$. As before, we take $P = ((t+1), (t+2), \ldots, (t+p-1))$. Visibly, if m is expressible in the form $\sum_i c_i p^{n^i}$, then $[m](P) \in X(\mathbb{F}_p(t))$. Conversely, for a general integer m, if $[m](P) \in X(\mathbb{F}_p(t))$, then because *a fortiori* $[m](P) \in X'(\mathbb{F}_p(t))$ we may express m as a sum of ℓ' powers of p. Then the preimage of $[m](P)$ under the map π from (24) consists of sequences of the form $\left(t^{p^{n_1}}, \ldots, t^{p^{n_{\ell'}}}\right)$. Since $[m](P)$ is also in the image of ν, the exponents must repeat c_1 times, and then c_2 times and so on, so that m may be expressed in the form $\sum_{j=1}^{\ell} c_j p^{n_j}$. □

Combining Propositions 4.2 and 4.3 we deduce Theorem 1.4 announced in the introduction.

5. A diophantine result

The following result is key for our proofs of Theorems 1.2 and 1.3.

Theorem 5.1. *Let $\{u_n\}_{n\in\mathbb{N}_0}$ be a linear recurrence sequence, let p be a prime number, let $m \in \mathbb{N}$, let $c_1, \dots, c_m \in \mathbb{Z}$ and let $k_1, \dots, k_m \in \mathbb{N}_0$.*

(A) *If p is multiplicatively independent with respect to each one of the characteristic roots of the linear recurrence sequence $\{u_n\}$ (i.e., for each characteristic root λ of $\{u_n\}$ and for any integers r and s, if $\lambda^r = p^s$, then $r = s = 0$), then the set of all $n \in \mathbb{N}_0$ for which there exist some $n_1, \dots, n_m \in \mathbb{N}_0$ such that*

$$u_n = c_1 p^{k_1 n_1} + \cdots + c_m p^{k_m n_m} \tag{29}$$

is a finite union of arithmetic progressions. (As always when dealing with an arithmetic progression $\{an+b\}_{n\in\mathbb{N}_0}$, we allow the possibility that $a = 0$, in which case, the arithmetic progression becomes a singleton.)

(B) *If $m \leq 2$, then the set of all $n \in \mathbb{N}_0$ for which there exist some $n_1, n_2 \in \mathbb{N}_0$ such that $u_n = c_1 p^{k_1 n_1} + c_2 p^{k_2 n_2}$ is a union of finitely many arithmetic progressions along with finitely many sets of the form*

$$\left\{ d_0 + d_1 p^{\ell_1 n_1} + d_2 p^{\ell_2 n_2} : n_1, n_2 \in \mathbb{N}_0 \right\}, \tag{30}$$

for some rational numbers d_0, d_1, d_2, and some non-negative integers ℓ_1, ℓ_2. (In particular, if $\ell_1 = \ell_2 = 0$, the set from (30) is a singleton.)

Remark 5.2. The proof presented below yields much more than required for the present purposes; indeed, we can conclude finiteness of the set of solutions except in a few well-described cases.

In particular, the proof for Part (B) implicitly gives that only the cases when u_n is essentially a polynomial with at most two distinct roots may produce infinitely many solutions, provided $k_i \neq 0$ for $i = 1, 2$ in Theorem 5.1 (B) (as we may clearly assume).

We have not pursued in obtaining and stating optimal conclusions, because in the first place this is not needed by the present application and anyway the interested reader shall readily see what can be extracted from the arguments.

We split our proof of Theorem 5.1 into the two parts of its conclusion.

Proof of Theorem 5.1, part (A). We prove part (A), showing how this follows directly from a theorem of M. Laurent, whose statement we borrow from W.M. Schmidt's presentation [Sch03] (see Thm. 7.1 therein).

We write u_n as an exponential polynomial (as in Section 2.3):

$$u_n = \sum_{i=1}^{s} P_i(n) r_i^n, \tag{31}$$

where the P_i are nonzero polynomials and the $r_i \in \mathbb{C}^*$ are pairwise distinct. For our purpose we may and shall assume that all the involved numbers are algebraic numbers.[1]

In proving the theorem we may partition $\mathbb{N}_0$ into arithmetical progressions of any prescribed modulus and hence we may assume without loss of generality that the recurrence is non-degenerate (i.e. no ratio r_i/r_j is a root of unity different from 1).

Under this assumption, we prove that in fact we have only finitely many solutions.

We write our equation as

$$\sum_{i=1}^{s} P_i(n) r_i^n - \sum_{j=1}^{m} c_j p^{k_j n_j} = 0, \tag{32}$$

where m, c_j, k_j are fixed. So our variables are $n, n_1, \dots, n_m$, which are supposed to vary in $\mathbb{N}_0$. For each solution we may partition the $s+m$ terms on the left side into subsets such that the sum over each subset vanishes; we may also suppose that each subset is minimal with respect to this property.

Since the number of possible partitions is finite, we may suppose on reducing s, m (but still assuming $s > 0$) that no proper subsum of the left side of (32) vanishes.

In this situation, Laurent's theorem takes into account the subgroup of $\mathbb{Z}^{m+1}$ consisting of the integer vectors $(a_0, a_1, \dots, a_m)$ for which,

$$r_\mu^{a_0} = r_\nu^{a_0}, \qquad r_\mu^{a_0} = p^{k_j a_j}, \tag{33}$$

for each $\mu, \nu \in \{1, \dots, s\}$ and each $j = 1, \dots, m$. The equations on the left of (33) may give no information, since s could be possibly 1, but the assumption on multiplicative independence of p and any of the roots r_i, applied to the set of equations on the right of (33), yields that $a_0 = a_1 = \ldots = a_m = 0$, i.e. our group reduces to 0.

Then Laurent's theorem asserts that the set of solutions is indeed finite, as required. □

Remark 5.3. It is to be observed that, given that u_n is non-degenerate, in order to obtain finiteness we used merely the existence of *one* of the roots r_i multiplicatively independent of p. It may thus seem that the stronger assumption of the independence for *all* roots is not needed. The point is however that in going to the non-degenerate case the assumption could be lost if it only held for a subset of the roots.

Proof of Theorem 5.1, part (B). This case is treated by using implicitly the Subspace Theorem (as is the case for Laurent's theorem). The technique has been applied in several papers of the first and fourth authors; see e.g. [CZ00]. This method works here as well; however, unfortunately we cannot directly appeal to the results proved before, because of slight differences in

[1] The case when this is not verified may be actually treated in a simpler way.

the assumptions and context. Therefore we develop again the same technique for the case in question. In short, this consists of expanding the relevant solutions in convergent power series in several variables, and then suitably applying the Subspace Theorem to the approximations so derived, using each time a suitable absolute value. At least we shall not need to repeat the use of the Subspace Theorem, and shall use instead a theorem proved in [CZ05]. The need that the variables x_i appearing in [CZ05] are such that the ratios $\log|x_i|/\log|x_j|$ be bounded above and below by fixed positive numbers (for the relevant absolute values) forces us to separate the proof into two cases, using an archimedean and a p-adic absolute value respectively.

As before we can argue on separate arithmetical progressions and thus we can assume at the outset that u_n is non degenerate.

Arguing as before (see also Remark 5.3) we can assume that each of the roots r_i is multiplicatively dependent with p (otherwise we may apply Laurent's theorem as before). Also, we may multiply everywhere by a power p^{An}. So, moving again along each among finitely many arithmetical progressions of n, we may write

$$r_i = p^{b_i}, \qquad 0 \le b_1 < b_2 < \ldots < b_s,$$

for integers b_i. Note that if some b_i were negative, then equation (29) becomes trivial.

On changing slightly the notation, we may write $k_1 = k_2 = 1$ and assume that for our solutions we have $0 \le n_1 \le n_2$ (and that n_1, n_2 are divisible by certain fixed integers k_1, k_2). We may also suppose that $u_n \neq 0$.

Let $v = v_p$ be the p-adic order function, extended in some way to a number field containing the relevant quantities.

The equation gives $v(c_1p^{n_1} + c_2p^{n_2}) \ge b_1n + O(1)$, so we may assume that $n_1, n_2 \ge b_1n + O(1)$. Then, dividing out by p^{b_1n} we reduce to the case $b_1 = 0$.

Now, $v(P_1(n) - c_1p^{n_1} - c_2p^{n_2}) \ge b_2n + O(1)$. If $P_1(n) - c_1p^{n_1} - c_2p^{n_2} \neq 0$ we deduce successively that $n_2 \ge b_2n + O(1)$ and then $n_1 \ge b_2n + O(1)$, which would imply $v(P_1(n)) \gg n$, which is inconsistent for large n.

Therefore

$$P_1(n) = c_1p^{n_1} + c_2p^{n_2}. \tag{34}$$

Implicitly this implies $s = 1$, and anyway this is the equation we shall deal with from now on.

For a given solution, we shall write

$$q := c_1p^{n_1} + c_2p^{n_2},$$

and we shall assume that n is large enough to justify the subsequent approximations. So, q shall also be large and therefore $n_2 = \max\{n_1, n_2\}$ shall be large as well.

We write $d := \deg P_1 > 0$.

We split the analysis into two similar cases, according as $n_1 < n_2/2$ or not.

Case I. Suppose first $n_1 < n_2/2$, so $\ell := n_2 - n_1 > n_2/2$. In equation (34), we expand in a Puiseux series for n at ∞ in terms of q:

$$n = q^{1/d} \sum_{r=0}^{\infty} \gamma_r q^{-r/d}, \tag{35}$$

where γ_r are certain coefficients depending only on P_1. Of course we tacitly mean that some definite branch has been chosen for the d-th root.

In turn, we may write $q^{-r/d} = c_2^{-r/d} p^{-rn_2/d} \left(1 + \frac{c_1}{c_2} p^{-\ell}\right)^{-r/d}$ and expand the factor on the right by the binomial theorem. Doing that for all $r \geq 0$ in (35) we may write

$$n = p^{n_2/d} f(p^{-n_2/d}, p^{-\ell}), \tag{36}$$

where $f(x,y) := \sum_{a,b\geq 0} \sigma_{a,b} x^a y^b$ is a certain power series with coefficients in a suitable number field, converging for x, y in a region $\max\{|x|, |y|\} \leq \rho$ for a sufficiently small $\rho > 0$.

We apply to this series and solutions Theorem 1 of the paper [CZ05] (written by two of the authors), on taking therein K a number field containing all relevant numbers, S the set of places of K which are either archimedean or lie above p, and the sequence of points $\mathbf{x} := (x_1, x_2) = \left(p^{-n_2/d}, p^{-\ell}\right)$.

In the Case I that we are treating we also choose ν as a complex absolute value for which the identity (36) holds.

Note that $f(\mathbf{x}) = np^{-n_2/d}$ is an S-integer, so assumption (3) for [CZ05, Theorem 1] holds. Also, the coordinates of $\mathbf{x}$ are S-units, so another of the assumptions in [CZ05, Theorem 1] indeed holds. Further, we have $h(\mathbf{x}) \asymp n_2 \asymp -\log|x_1|_\nu \asymp -\log|x_2|_\nu$, and this takes care of all other required inequalities.

The conclusion of the theorem delivers finitely many algebraic cosets $\mathbf{u}_1 H_1, \ldots, \mathbf{u}_\ell H_\ell$ of $\mathbb{G}_m^2$, whose union contains all of our points $\mathbf{x}$, and such that the restriction of f to each $\mathbf{u}_i H_i$ is a polynomial. Also, the identities (36) express the integers n in term of these polynomials and points.

Suppose first that one of the cosets is the whole $\mathbb{G}_m^2$. Then f is a polynomial in its arguments, and (36) says it satisfies $P_1(x^{-1} f(x,y)) = (c_1 y + c_2) x^{-d}$. This entails that $d = 1$, so $P_1(n) = an + b$ and $af(x,y) = c_1 y + c_2 - bx$. This yields the required shape for the solutions n.

Suppose now that each of the cosets is proper. We can focus on the cosets of dimension 1 and containing infinitely many elements $\mathbf{x}$, the others giving rise to finitely many solutions. Since $\mathbf{x}$ tends to zero the coset may be parametrized by $x = t^a, y = \mu t^b$, with coprime integers $a, b > 0$ and a nonzero constant μ. The restriction of f to this coset corresponds to $f(t^a, \mu t^b)$, which is thus a polynomial, denoted $\phi(t)$. We also have

$$P_1(t^{-a}\phi(t)) = c_1 \mu t^{b-da} + c_2 t^{-da}.$$

We see that $\phi(0) \neq 0$ and if $c := \deg \phi$ we have $b = dc$. Thus the left side is a Laurent-polynomial in t^d, and is thus invariant by $t \mapsto \zeta t$ with any d-th root of unity ζ. We could exploit this fact through Galois groups, but we choose a more direct way to describe the situation completely.

Our solutions are obtained by substitutions $t = p^{-n_2/(da)}$ and we have

$$da\ell = bn_2,\ n_2 - \frac{bn_2}{da} = n_1 \geq 0,$$

so $b < da$. Setting $1/t$ in place of t and changing slightly notation, we may write

$$P_1(\psi(t)) = c_1 t^{du} + c_2 t^{da}, \tag{37}$$

where $0 \leq u = a - c < a$ and where $\psi(t) = t^a \phi(t^{-1})$. Note that $\psi(t)$ is necessarily a polynomial, of degree a.

If $d = 1$ our conclusion follows at once, so suppose $d > 1$. If ρ is a root of P_1 of multiplicity $\mu > 1$ then necessarily $\psi(t) - \rho$ equals a constant times t^{du}, since the right side of (37) has only $t = 0$ as a multiple root. This again yields the required representations for n.

Suppose then that P_1 has no multiple roots. Still, t^{du} shall divide exactly one factor $\psi(t) - \rho$, so $du \leq \deg \psi = a$.

Let now $Q(x) = P(x + \beta)$ where β is chosen so that Q has vanishing second coefficient, and let $\xi(t) = \psi(t) - \beta$, so $Q(\xi(t)) = P_1(\psi(t))$. For δ the leading coefficient of Q, we have

$$\deg(\delta \xi(t)^d - c_2 t^{da}) \leq \max\{d\ell, (d-2)\deg \xi\} \leq \max\{a, (d-2)a\}. \tag{38}$$

However $\delta \xi(t)^d - c_2 t^{da}$ is a product of d terms of the shape $\gamma_1 \xi(t) - \gamma_2 \zeta t^a$, where ζ runs over the d-th roots of unity, and at most one term has degree $< a$. Hence either $\delta \xi(t)^d - c_2 t^{da}$ vanishes, or it has degree $\geq (d-1)a$, and in case of equality one of the factors has to be constant.

Comparing with the inequality (38), in any case again we find that $\psi(t)$ is of the shape $\gamma t^a + \gamma'$, and we conclude as before.

Case II. We are left with the case when $n_1 \geq n_2/2$. Now we argue in an entirely similar way, but expanding for n at $q = 0$ and using a p-adic absolute value in place of an archimedean one; however a few supplementary arguments are needed because when n_1/n_2 is very near to 1 the Puiseux expansion may not obey the needed conditions. To dispose of this difficulty we argue as follows.

If $n_2 - n_1$ is bounded for infinitely many solutions, then we fall essentially into the equation $P_1(n) = c_3 p^{n_1}$; this is standardly known, and may be solved even effectively for given P_1, p (there are only finitely many solutions unless P_1 is a power of a linear polynomial). So we assume that $n_2 - n_1$ tends to infinity for our solutions.

First, $P_1(x)$ may be supposed clearly with rational coefficients, and let us consider powers $Q(x)^m$ dividing it exactly, where Q is an irreducible polynomial in $\mathbb{Q}[x]$ and $m \geq 1$. Now, one such factor at least will be such

that $v(Q(n)^m) = n_1 + O(1)$, while we must have bounded p-adic order for the other factors.

Suppose first that there are no other non constant factors, so $P_1 = cQ^m$; then $c_1 + c_2 p^{n_2 - n_1}$ must be an m-th power, up to a factor taken from a finite set. By well-known results this leads to only finitely many solutions if $m > 1$, so let us assume $m = 1$. In this case there is no ramification above $q = 0$, so we may expand the solutions of $P_1(n) = q$ at $q = 0$ in a power series $n = \sum_{r=0}^{\infty} \gamma_r q^r$ converging in any absolute value for which q is small enough.[2] We choose a p-adic place ν of a number field K containing all the coefficients γ_r. Note that since we have no ramification, the powers of q which appear are integers, and we may expand $q^r = (c_1 p^{n_1} + c_2 p^{n_2})^r$ with the binomial theorem, to obtain a series $f(x, y) = \sum_{a,b \geq 0} \sigma_{a,b} x^a y^b$, with $n = f(p^{n_1}, p^{n_2})$ in the valuation ν. Now the proof proceeds exactly as in Case I (actually even with the slight simplification of having no fractional powers involved). (This case actually falls as part of a result proved in [CZ00].)

Suppose now that there is some other non-constant factor. Then, since the product of the other factors contributes at most essentially $p^{n_2 - n_1}$, we find $p^{n_2 - n_1} \gg n$, whereas $p^{n_2} \ll n^d$, so $n_1 \leq n_2(1 - d^{-1}) + O(1)$. With this inequality, we can use a Puiseux expansion at $q = 0$, even if there is ramification. Corresponding to each branch, we have an expansion $n = \sum_{r \geq 0} \gamma_r q^{r/e}$ for a suitable integer $e > 0$, converging at any p-adic place ν for small enough $|q|_\nu$, i.e. for large enough n_1. We can further expand the powers $q^{r/e}$ as $q^{r/e} = c_1^{r/e} p^{r n_1/e} (1 + (c_2/c_1) p^{n_2 - n_1})^{r/e}$, using the binomial theorem on the right. The fact that $n_2 - n_1 \gg n_2$ enables us to obtain a sufficiently fast convergence in order to apply again Theorem 1 of [CZ05] as in Case I. This shall lead to the sought conclusion as above. □

Remark 5.4. It will be noted that for $n_1 > \epsilon n_2$ (for any fixed $\epsilon > 0$), we can use either argument for both cases. Under such type of inequalities actually the arguments work for the representations of u_n as the sum of any prescribed number of terms of the shape $c_i p^{n_i}$. It is the lack of such inequalities that prevent the proof to go through for the general case; so already for three terms one meets problems if n_1/n_3 tends to 0 and n_2/n_3 tends to 1 through a sequence of solutions. See [CZ13] for devices to overcome this kind of difficulty in special cases.

Also, the expansions used in the proof might be explained in geometric terms, after suitable blow-ups.

6. Proof of Theorems 1.2 and 1.3

Using Theorem 5.1, we deduce our main results.

[2] Several power series may appear, corresponding to the various branches, represented by the roots of $P_1 = 0$.

Proof of Theorem 1.2. Using Theorem 3.2, we know that the set

$$S = \{n \in \mathbb{N}_0 \colon \Phi^n(\alpha) \in V\}$$

(where $\Phi : \mathbb{G}_m^N \longrightarrow \mathbb{G}_m^N$ is a regular self-map and $V \subset \mathbb{G}_m^N$ is a surface) is a finite union of generalized F-arithmetic sequences. Since the minimal polynomial $P_{\min,F} \in \mathbb{Z}[x]$ of the Frobenius has a unique root equal to p, then each such generalized F-arithmetic sequence is the intersection of finitely many F-arithmetic sequences, each one of them consisting of all non-negative integers n which belong to a suitable arithmetic progression and furthermore, for which there exist some $m \in \mathbb{N}_0$ and some $n_1, \ldots, n_m \in \mathbb{N}_0$ such that

$$u_n = c_1 p^{k_1 n_1} + \cdots + c_m p^{k_m n_m}, \tag{39}$$

for some given linear recurrence sequence $\{u_n\}$, some given integers c_i and some given non-negative integers k_i. Furthermore, by Theorem 3.2 (1), since $\dim(V) = 2$, we have that at most two of the k_i's in equation (39) are nonzero. So, at the expense of replacing u_n by $u_n - c$ (for a suitable integer), we may assume $m = 2$. Then Theorem 5.1 (B) yields that each such F-arithmetic sequence is a union of finitely many arithmetic progressions and finitely many p-sets of the form (30). Then Propositions 2.6 and 2.7 yield that these finitely many intersections of F-arithmetic sequences are once again a finite union of arithmetic progressions and finitely many p-sets. □

Proof of Theorem 1.3. Again using Theorem 3.2, we obtain that the set S consisting of all $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V$ is a finite union of generalized F-arithmetic sequences, and furthermore, each such generalized F-arithmetic sequence is a finite intersection of finitely many F-arithmetic sequences, each one of them consisting of all non-negative integers n belonging to a suitable arithmetic progression and furthermore, for which there exist $n_1, \ldots, n_m \in \mathbb{N}_0$ such that

$$u_n = c_1 p^{k_1 n_1} + \cdots + c_m p^{k_m n_n}, \tag{40}$$

for some given linear recurrence sequence $\{u_n\}$, some given $m \in \mathbb{N}_0$, some given integers c_i and some given non-negative integers k_i. As shown in Theorem 3.2 (2), since $\Phi : \mathbb{G}_m^N \longrightarrow \mathbb{G}_m^N$ is a group endomorphism, the characteristic roots of the linear recurrence sequence $\{u_n\}$ from (40) are positive integer powers of the roots of the minimal polynomial $P_{\min,\Phi} \in \mathbb{Z}[x]$ of Φ. Now, the hypothesis regarding Φ from Theorem 1.3 yields that no root of $P_{\min,\Phi}$ is multiplicatively dependent with the prime p; then Theorem 5.1 (A) finishes the proof of our result. Indeed, if $P_{\min,\Phi}$ were to have a root λ which is multiplicatively dependent with the prime p, then we would have that for some iterate Φ^r (for a suitable $r \in \mathbb{N}$) there is a root of its minimal polynomial $P_{\min,\Phi^r} \in \mathbb{Z}[x]$ which equals p^s for some $s \in \mathbb{N}_0$. Letting $G = \ker(\Phi^r - p^s \mathrm{Id})$, where Id is the identity morphism on $\mathbb{G}_m^N$, we obtain that G is a positive dimensional algebraic subgroup of $\mathbb{G}_m^N$ and the induced action of Φ on G is given by a power of the Frobenius, contradiction.

This concludes the proof of Theorem 1.3. □

References

[BG06] E. Bombieri and W. Gubler, *Heights in diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[BGT16] J. P. Bell, D. Ghioca, and T. J. Tucker, *The Dynamical Mordell-Lang Conjecture*, Mathematical Surveys and Monographs **210**, American Mathematical Society, Providence, RI, 2016, xiv+280 pp.

[CZ00] P. Corvaja and U. Zannier, *On the Diophantine equation* $f(a^m, y) = b^n$, Acta Arith. **94** (2000), no. 1, 25-40.

[CZ05] P. Corvaja and U. Zannier, *S-unit points on analytic hypersurfaces*, Ann. Sci. Èc. Norm. Sup. **38** (2005), 76–92.

[CZ13] P. Corvaja and U. Zannier, *Finiteness of odd perfect powers with four nonzero binary digits*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 2, 715-731.

[Der07] H. Derksen, *A Skolem-Mahler-Lech theorem in positive characteristic and finite automata*, Invent. Math. **168** (2007), no. 1, 175-224.

[DM12] H. Derksen and D. Masser, *Linear equations over multiplicative groups, recurrences, and mixing I*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 5, 1045-1083.

[Eis95] D. Eisenbud, *Commutative algebra: With a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, New York, 1995.

[Fal94] G. Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Albano Terme, 1991), Perspective in Math., vol. 15, Academic Press, San Diego, 1994, pp. 175–182

[Ghi08] D. Ghioca, *The isotrivial case in the Mordell-Lang theorem*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3839-3856.

[Ghi] D. Ghioca, *The dynamical Mordell-Lang conjecture in positive characteristic*, Trans. Amer. Math. Soc., to appear (2018), 18 pp.

[GT09] D. Ghioca and T. J. Tucker, *Periodic points, linearizing maps, and the dynamical Mordell-Lang problem*, J. Number Theory **129** (2009), 1392–1403.

[GTZ11] D. Ghioca, T. J. Tucker, and M. E. Zieve, *The Mordell-Lang question for endomorphisms of semiabelian varieties*, J. Theor. Nombres Bordeaux **23** (2011), 645–666.

[Hru96] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), no. 3, 667-690.

[Lau84] M. Laurent, *Équations diophantiennes exponentielles*, Invent. Math. **78** (1984), no. 2, 299-327.

[Lec53] C. Lech, *A note on recurring series*, Ark. Mat. **2** (1953), 417–421.

[Mah56] K. Mahler, *On the Taylor coefficients of rational functions*, Proc. Cambridge Philos. Soc. **52** (1956), 39-48.

[Mas04] D. Masser, *Mixing and linear equations over groups in positive characteristic*, Israel J. Math. **142** (2004), 189–204.

[Mil] J. Milne, *Abelian varieties*, lecture notes available online.

[MS04] R. Moosa and T. Scanlon, *F-structures and integral points on semiabelian varieties over finite fields*, Amer. Journal of Math. **126** (2004), 473–522.

[Nel17] K. Nelson, *Two special cases of the dynamical Mordell-Lang conjecture*, Master's thesis, University of British Columbia, March 2017.

[SY14] T. Scanlon and Y. Yasufuku, *Exponential-polynomial equations and dynamical return sets*, Int. Math. Res. Not. IMRN **2014** (2014), 4357–4367.

[Sch03] W. Schmidt, *Linear recurrence sequences*, Diophantine Approximation (Cetraro, Italy, 2000), Lecture Notes in Math. 1819, Springer-Verlag Berlin Heidelberg, 2003, pp. 171–247.

[Sko34] T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, Comptes Rendus Congr. Math. Scand. (Stockholm, 1934) 163–188.

[Voj96] P. Vojta, *Integral points on subvarieties of semiabelian varieties, I*, Invent. Math. **126** (1996), 133–181.

[Zan09] U. Zannier, *Lecture notes on Diophantine analysis. With an appendix by Francesco Amoroso*, Scuola Normale Superiore di Pisa (Nuova Serie) **8**. Edizioni della Normale, Pisa, 2009. xvi+237 pp.

Pietro Corvaja, Dipartimento di Scienze Matematiche, Informatiche e Fisiche, Università di Udine, via delle Scienze, 206, 33100 Udine, Italy
E-mail address: pietro.corvaja@uniud.it

Dragos Ghioca, Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver, BC V6T 1Z2, Canada
E-mail address: dghioca@math.ubc.ca

Thomas Scanlon, University of California, Berkeley, Mathematics Department, Evans Hall, Berkeley, CA 94720-3840, USA
E-mail address: scanlon@math.berkeley.edu

Umberto Zannier, Scuola Normale Superiore, Piazza dei Cavalieri, 7, 56126 Pisa, Italy
E-mail address: u.zannier@sns.it