

THE DYNAMICAL MORDELL-LANG CONJECTURE IN POSITIVE CHARACTERISTIC

DRAGOS GHIOCA

ABSTRACT. Let K be an algebraically closed field of prime characteristic p , let $N \in \mathbb{N}$, let $\Phi : \mathbb{G}_m^N \rightarrow \mathbb{G}_m^N$ be a self-map defined over K , let $V \subset \mathbb{G}_m^N$ be a curve defined over K , and let $\alpha \in \mathbb{G}_m^N(K)$. We show that the set $S = \{n \in \mathbb{N} : \Phi^n(\alpha) \in V\}$ is a union of finitely many arithmetic progressions, along with a finite set and finitely many p -arithmetic sequences, which are sets of the form $\{a + bp^{kn} : n \in \mathbb{N}\}$ for some $a, b \in \mathbb{Q}$ and some $k \in \mathbb{N}$. We also prove that our result is sharp in the sense that S may be infinite without containing an arithmetic progression. Our result addresses a positive characteristic version of the dynamical Mordell-Lang conjecture and it is the first known instance when a structure theorem is proven for the set S which includes p -arithmetic sequences.

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 $\Phi \circ \dots \circ \Phi$, where Φ^0 denotes the identity map on X . If $\alpha \in X$, we define the orbit $\mathcal{O}_\Phi(\alpha) := \{\Phi^n(\alpha) : n \in \mathbb{N}_0\}$.

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 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

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

is a finite union of arithmetic progressions (see [GT09, Conjecture 1.7] along with the earlier work of Denis [Den94] and Bell [Bel06]). Considering X a semiabelian variety and Φ the translation by a point $x \in X(K)$, one recovers the cyclic case in the classical Mordell-Lang conjecture from the above stated dynamical Mordell-Lang Conjecture; we refer the readers to [BGT16] for a survey of recent work on the dynamical Mordell-Lang conjecture.

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,

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

Key words and phrases. Dynamical Mordell-Lang problem, endomorphisms of algebraic tori over fields of characteristic p .

The author has been partially supported by a Discovery Grant from the National Science and Engineering Board of Canada.

Example 3.4.5.1] or our Example 1.4). Similar to the classical Mordell-Lang conjecture in characteristic p , one has to take into account varieties defined over finite fields. So, motivated by the structure theorem of Moosa-Scanlon describing in terms of F -sets the intersection of a subvariety of a semiabelian variety (in positive characteristic) with a finitely generated group (see [MS04] and also [Ghi08]), the following conjecture was proposed in [BGT16, Conjecture 13.2.0.1].

Conjecture 1.1 ((Ghioca-Scanlon) 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 $S := S(X, \Phi, V, \alpha)$ of integers $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V(K)$ is a union of finitely many arithmetic progressions along with finitely many sets of the form

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

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

Clearly, the set S may contain infinite arithmetic progressions if V contains some periodic subvariety under the action of Φ which intersects $\mathcal{O}_\Phi(\alpha)$. On the other hand, it is possible for S to contain nontrivial sets of the form (1) (where m is even larger than 1; see Example 1.2).

Example 1.2. Let $p > 2$, let $K = \mathbb{F}_p(t)$, let $X = \mathbb{G}_m^3$, let $\Phi : \mathbb{G}_m^3 \longrightarrow \mathbb{G}_m^3$ given by $\Phi(x, y, z) = (tx, (1+t)y, (1-t)z)$, let $V \subset \mathbb{G}_m^3$ be the hyperplane given by the equation $y + z - 2x = 2$, and let $\alpha = (1, 1, 1)$. Then one easily checks that the set S from Conjecture 1.1 consists of all numbers of the form $p^{n_1} + p^{n_2}$ for $n_1, n_2 \in \mathbb{N}_0$.

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 even harder than the original Conjecture 1.1.

In [BGT15, Theorem 1.4] (see also [Pet15]), it is proven that the set S from Conjecture 1.1 is a union of finitely many arithmetic progressions along with a set of Banach density 0. However, Conjecture 1.1 predicts a much more precise description of the set S . The only nontrivial case when Conjecture 1.1 was known to hold prior to our present paper is the case of group endomorphisms Φ of algebraic tori $X = \mathbb{G}_m^n$ under the additional assumption that the action of Φ on the tangent space at the identity of X is given by a diagonalizable matrix (see [BGT16, Proposition 13.3.0.2]). Under these assumptions, one proves that the set S consists only of finitely many arithmetic progressions, i.e., the more complicated sets of the form (1) *do not appear*. In this paper we prove the first important partial result towards Conjecture 1.1 by showing it holds for any curve V contained in \mathbb{G}_m^N endowed with a regular self-map Φ (not necessarily a group endomorphism). Since our result has no restriction on Φ , our proof is more complicated than the proof of [BGT16, Proposition 13.3.0.2] (knowing that Φ is a group endomorphism with its Jacobian at the identity being a diagonalizable matrix simplifies significantly the arguments since the sets of the form (1) do not appear in the conclusion). In our

Theorem 1.3, we encounter sets of the form (1) (see also Example 1.4 which shows that our conclusion is sharp).

Theorem 1.3. *Let K be an algebraically closed field of characteristic p , let $N \in \mathbb{N}$, let $V \subset \mathbb{G}_m^N$ be an irreducible curve and $\Phi : \mathbb{G}_m^N \rightarrow \mathbb{G}_m^N$ be a regular self-map both defined over K , and let $\alpha \in \mathbb{G}_m^N(K)$. Then the set S of all $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V(K)$ is either a finite union of arithmetic progressions, or a finite union of sets of the form*

$$(2) \quad \{ap^{kn} + b : n \in \mathbb{N}_0\},$$

for some $a, b \in \mathbb{Q}$ and $k \in \mathbb{N}_0$.

We note that if $k = 0$ in (2), then the corresponding set is a singleton; hence, both options (arithmetic progressions and sets as in (2)) allow for the possibility that S may consist of finitely many elements (perhaps, along with finitely many infinite arithmetic progressions or finitely many sets as in (2)). Proposition 2.3 allows us to prove the more precise conclusion in Theorem 1.3 compared to the one formulated in Conjecture 1.1. We show in the example below that indeed, it is possible in equation (2) from the conclusion of Theorem 1.3 that a and b are *not integers*.

Example 1.4. Let p be a prime number, let $V \subset \mathbb{G}_m^2$ be the curve defined over $\mathbb{F}_p(t)$ given by the equation $tx + (1-t)y = 1$, let $\Phi : \mathbb{G}_m^2 \rightarrow \mathbb{G}_m^2$ be the endomorphism given by $\Phi(x, y) = (t^{p^2-1} \cdot x, (1-t)^{p^2-1} \cdot y)$, and let $\alpha = (1, 1)$. Then the set S of all $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in V$ is

$$\left\{ \frac{1}{p^2-1} \cdot p^{2n} - \frac{1}{p^2-1} : n \in \mathbb{N}_0 \right\}.$$

Trying to extend Theorem 1.3 seems to be impossible at this moment. On one hand, if we work with an arbitrary quasiprojective variety X , then Conjecture 1.1 is expected to be very difficult since even its counterpart in characteristic 0 is only known to hold in special cases, and generally, when it holds, its proof involves methods which fail in positive characteristic, such as the so-called *p-adic arc lemma* (see [BGT16, Chapter 4] and its main application from [BGT10] to the dynamical Mordell-Lang conjecture for étale endomorphisms in characteristic 0). On the other hand, even if X is assumed to be \mathbb{G}_m^N and Φ is a group endomorphism, unless one assumes another hypothesis (either on Φ as in [BGT16, Chapter 13], or on V as in Theorem 1.3), Conjecture 1.1 is expected to be very difficult. Trying to solve it, even in the case of arbitrary subvarieties of $X = \mathbb{G}_m^N$, it leads to difficult questions involving polynomial-exponential equations (see Remark 4.3 and the references therein). Also, in Remark 4.3 we explain the difficulties one would have to overcome if one would try to extend Theorem 1.3 even to the case of curves contained in an arbitrary semiabelian variety defined over a finite field.

We sketch below the plan of our paper. In Section 2 we discuss the classical Mordell-Lang problem for algebraic tori in characteristic p , by stating the results of Moosa-Scanlon [MS04] and of Derksen-Masser [DM12] and then explaining their connections to Conjecture 1.1 (we also note the result of Derksen [Der07] in the same spirit to [MS04, DM12]). In Section 3 we introduce the so-called *p*-arithmetic sequences, i.e., sets of the form (2) and discuss properties of these sequences including in the larger context of linear recurrence sequences. Then we proceed to prove our main result in Section 4.

Acknowledgments. We thank Khoa Nguyen and Umberto Zannier for several useful conversations. We also thank the referee for his/her comments.

2. THE MORDELL-LANG PROBLEM IN POSITIVE CHARACTERISTIC

In the classical Mordell-Lang problem in characteristic 0, Faltings [Fal94] and Vojta [Voj96] proved that if an irreducible subvariety V of a semiabelian variety X intersects a finitely generated subgroup of X in a Zariski dense set, then V must be a translate of a connected algebraic subgroup of X . In particular, their result immediately yields a structure theorem for the intersection of any subvariety of X with any finitely generated subgroup.

Hrushovski [Hru96] gave a complete description of all subvarieties V of semiabelian varieties X defined over fields K of characteristic $p > 0$ with the property that for some finitely generated $\Gamma \subset X(K)$, the intersection $V(K) \cap \Gamma$ is Zariski dense in V . However, since Hrushovski's result [Hru96] is quite intricate, it does not give a structure theorem for the intersection of an arbitrary subvariety with an arbitrary finitely generated subgroup of X . In the case when X is a semiabelian variety defined over a finite field, Moosa and Scanlon [MS04] (see also [Ghi08]) gave a complete description of the intersection $V(K) \cap \Gamma$ in terms of the so-called F -sets, where F is the Frobenius endomorphism of X . In the case $X = \mathbb{G}_m^N$, using a different method, Derksen and Masser [DM12] improved the result from [MS04] by showing that the intersection $V(K) \cap \Gamma$ can be computed effectively using heights. In order to state their structure theorem for the intersection $V(K) \cap \Gamma$ (see Theorem 2.2), we introduce first the notion of F -sets (which also motivated the statement of Conjecture 1.1).

Definition 2.1. *Let $N \in \mathbb{N}$, let K be an algebraically closed field of characteristic p , and let $\Gamma \subseteq \mathbb{G}_m^N(K)$ be a finitely generated subgroup.*

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

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

where $\alpha_1, \dots, \alpha_m \in \mathbb{G}_m^N(K)$ and $k_1, \dots, k_m \in \mathbb{N}_0$.

- (b) *An F -set in Γ is a set of the form $C \cdot \Gamma'$ where C is a product of F -orbits in Γ , and $\Gamma' \subseteq \Gamma$ is a subgroup, while in general, for two sets $A, B \subset \mathbb{G}_m^N(K)$, then $A \cdot B$ is simply the set $\{a \cdot b : a \in A, b \in B\}$.*

The motivation for using the name F -set comes from the reference to the Frobenius corresponding to \mathbb{F}_p (lifted to an endomorphism F of \mathbb{G}_m^N) since an F -orbit $C(\alpha; k)$ is simply the orbit of a point in $\mathbb{G}_m^N(K)$ under F^k .

We note that allowing for the possibility that some $k_i = 0$ in the definition of a product of F -orbits, implicitly we allow a singleton be a product 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 $k_2 = \dots = k_m = 0$ then the corresponding product of F -orbits is simply a translate of the single F -orbit $C(\alpha_1; k_1)$. Finally, note that the F -orbit $C(\alpha; k)$ for $k > 0$ is finite if and only if $\alpha \in \mathbb{G}_m^N(\overline{\mathbb{F}_p})$.

Theorem 2.2 (Moosa-Scanlon [MS04], Derksen-Masser [DM12]). *Let $N \in \mathbb{N}$, let K be an algebraically closed field of characteristic p , let $V \subset \mathbb{G}_m^N$ be a subvariety*

defined over K and let $\Gamma \subset \mathbb{G}_m^N(K)$ be a finitely generated subgroup. Then $V(K) \cap \Gamma$ is a finite union of F -sets contained in Γ .

We note that the main result of [MS04] is stated using the notion of F -cycles; however, at the expense of allowing the base points of the F -orbits live outside of the group Γ (as in part (a) of Definition 2.1), then we obtain the description of the intersection $V(K) \cap \Gamma$ as in the conclusion of Theorem 2.2.

If V is an irreducible curve, one can deduce easily the following slightly more precise statement which will be used in the proof of Theorem 1.3.

Corollary 2.3. *With the notation from Theorem 2.2, if V is an irreducible curve, then the intersection $V(K) \cap \Gamma$ is either finite, or a coset of an infinite subgroup of Γ , or a finite union of translates of single F -orbits contained in Γ .*

Proof. Assume $V(K) \cap \Gamma$ is infinite. Then, according to Theorem 2.2, there exists an infinite F -set $C \cdot \Gamma'$ contained in the intersection $V(K) \cap \Gamma$. So, either the product C of F -orbits is infinite, or the subgroup Γ' of Γ is infinite.

If Γ' is infinite, then V must contain a coset $c \cdot \Gamma'$ (for some $c \in C$) and since V is an irreducible curve, then $V = c \cdot H$, where H is the Zariski closure of Γ' . Because Γ' is an infinite group, we conclude that H is a 1-dimensional algebraic subtorus; so, V is a coset of this algebraic subgroup of \mathbb{G}_m^N . In conclusion, the intersection $V \cap \Gamma$ must also be a coset of a subgroup of Γ ; more precisely, it equals $c \cdot (H \cap \Gamma)$.

Assume now that V is not a translate of an algebraic group, since in that case we get the desired conclusion; in particular, with the above notation, we also know that Γ' is a finite subgroup of Γ . Then the product of F -orbits C must be infinite. Assume C contains the product of at least two infinite F -orbits; note that if there is only one infinite F -orbit in C , then we may re-write $C \cdot \Gamma'$ so that it is the union of finitely many translates of single F -orbits, as desired in our conclusion. Therefore, a translate V' of V must contain the product of two infinite F -orbits:

$$C' := \left\{ \alpha_1^{p^{k_1 n_1}} \cdot \alpha_2^{p^{k_2 n_2}} : n_1, n_2 \in \mathbb{N}_0 \right\},$$

for some $k_1, k_2 \in \mathbb{N}$ and some $\alpha_1, \alpha_2 \in \mathbb{G}_m^N(K) \setminus \mathbb{G}_m^N(\overline{\mathbb{F}_p})$. In particular, because V' is an irreducible curve, we get that for each $n_1 \in \mathbb{N}_0$, the Zariski closure of the set

$$\left\{ \alpha_1^{p^{k_1 n_1}} \cdot \alpha_2^{p^{k_2 n_2}} : n_2 \in \mathbb{N}_0 \right\}$$

is actually the curve V' itself. But then the stabilizer W of V' in \mathbb{G}_m^N , i.e. the algebraic subgroup of \mathbb{G}_m^N consisting of all points $x \in \mathbb{G}_m^N$ such that $x \cdot V' \subset V'$ is positive-dimensional since it contains all points of the form $\alpha_1^{p^{k_1 n_1} - 1}$ for $n_1 \in \mathbb{N}_0$. Because V' is a curve, then V' must be a translate of W , and therefore V is a translate of an algebraic group, contradicting our assumption. So, in this case it must be that $V(K) \cap \Gamma$ is a finite union of cosets of single F -orbits.

This concludes the proof of Proposition 2.3. \square

2.1. Strategy for proving Theorem 1.3. Here we discuss briefly the strategy for proving our main result. We have two main ingredients for the proof of Theorem 1.3: on one hand, we have Theorem 2.2 along with its slight strengthening from Corollary 2.3 in the case of irreducible curves, and on the other hand, we have a result combining theory of arithmetic sequences and linear algebra (Theorem 4.1). In order to prove Theorem 1.3 we proceed as follows. With the notation as in Theorem 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 $\mathcal{O}_\Phi(\alpha)$. We use Corollary 2.3 and then intersect each F -set appearing in $V(K) \cap \Gamma$ with $\mathcal{O}_\Phi(\alpha)$ and apply Theorem 4.1. So, essentially our argument splits into two cases:

- (i) given a coset $c \cdot \Gamma'$ of a subgroup of Γ , we show that the set of $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in c \cdot \Gamma'$ is a finite union of arithmetic progressions; and
- (ii) given a translate C of a single F -orbit contained in Γ , we show that the set of $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in C$ is a union of finitely many arithmetic progressions along with finitely many sets of the form (2), i.e.,

$$(3) \quad \{ap^{kn} + b : n \in \mathbb{N}_0\},$$

for some given $a, b \in \mathbb{Q}$ and $k \in \mathbb{N}_0$. Sets such as the one from (3) will be called *p-arithmetic sequences* (see Definition 3.3). Then Proposition 2.4 delivers the more precise conclusion in Theorem 1.3.

Finally, we conclude this section by showing that for an irreducible curve V , if there exists an infinite arithmetic progression \mathcal{P} such that $\Phi^n(\alpha) \in V$ for each $n \in \mathcal{P}$, then the set S from the conclusion of Theorem 1.3 is a finite union of infinite arithmetic progressions. Actually, as we will see in Proposition 2.4, this conclusion holds in much higher generality than the hypotheses of Theorem 1.3.

Proposition 2.4. *Let X be a quasiprojective variety defined over an algebraically closed field K , let $\Phi : X \rightarrow X$ be an endomorphism, let $V \subseteq X$ be an irreducible curve, let $\alpha \in X(K)$, and let*

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

If S contains an infinite arithmetic progression, then S is a finite union of arithmetic progressions.

Proof. First we note that if α is preperiodic under the action of Φ , i.e., its orbit $\mathcal{O}_\Phi(\alpha)$ is finite, then the conclusion holds easily (see also [BGT16, Proposition 3.1.2.9]). So, from now on, we assume α is not preperiodic.

By our assumption, we know that there exist $a, b \in \mathbb{N}$ such that $\{an + b : n \in \mathbb{N}_0\} \subseteq S$. Since V is irreducible and α is not preperiodic, we conclude that V is the Zariski closure of the set $\{\Phi^{an+b}(\alpha) : n \in \mathbb{N}_0\}$, and in particular, we get that $\Phi^a(V) \subseteq V$. Therefore, for each $i \in \{0, \dots, a-1\}$, if there exists some $j \in \mathbb{N}_0$ such that $j \equiv i \pmod{a}$ and moreover, $\Phi^j(\alpha) \in V$, then $\{an + j : n \in \mathbb{N}_0\} \subset S$. In conclusion, S itself is a finite union of arithmetic progressions. \square

Remark 2.5. Actually, in Proposition 2.4, under the assumption that α is not preperiodic under Φ , if we let a_0 be the smallest positive integer such that there exist $j_1, j_2 \in \mathbb{N}_0$ such that $j_2 - j_1 = a_0$ and moreover, $\Phi^{j_1}(\alpha), \Phi^{j_2}(\alpha) \in V$, we obtain that the set S is itself a *single* infinite arithmetic progression of common difference a_0 . However, this more precise statement is not needed later in our proof.

3. ARITHMETIC SEQUENCES

In this section we prove various useful results regarding linear recurrence sequences (see Definition 3.1). Two special types of linear recurrence sequences which appear often in our paper are arithmetic progressions and *p*-arithmetic sequences (see Definition 3.3).

3.1. Linear recurrence sequences. We define next linear recurrence sequences which are essential in our proof.

Definition 3.1. *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*

$$(4) \quad u_{n+m} + c_{m-1}u_{n+m-1} + \dots + c_1u_{n+1} + c_0u_n = 0.$$

If $c_0 = 0$ in (4), 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

$$(5) \quad u_{n+m-k} + c_{m-1}u_{n+m-1-k} + \dots + c_ku_n = 0,$$

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 (5)); 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 (5)). The characteristic roots of a linear recurrence sequence as in (4) are the roots of the equation

$$(6) \quad x^m + c_{m-1}x^{m-1} + \dots + c_1x + c_0 = 0.$$

We let r_i (for $1 \leq i \leq s$) be the (nonzero) roots of the equation (6); then there exist polynomials $P_i(x) \in \mathbb{C}[x]$ such that for all $n \in \mathbb{N}_0$, we have

$$(7) \quad u_n = \sum_{i=1}^s P_i(n)r_i^n.$$

In general, as explained above, for an arbitrary linear recurrence sequence, the formula (7) holds for all n sufficiently large (more precisely, for all $n \geq m$ with the notation from (4)); 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 (7) (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 (7) and satisfying properties (i)-(ii) above are called *non-degenerate*. As an aside, we note that some authors do not require condition (i) in the definition of non-degenerate linear recurrence sequences. 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

$$(8) \quad u_{nM+\ell} = \sum_{i=1}^s P_i(nM + \ell)r_i^\ell (r_i^M)^n$$

and moreover, we can re-write the formula (8) 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 3.2. *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.*

3.2. A special type of linear recurrence sequences. We start by introducing the following notation.

Definition 3.3. *Let p be a prime number. We call a p -arithmetic sequence a set of the form*

$$\{ap^{kn} + b : n \in \mathbb{N}_0\},$$

for some $a, b \in \mathbb{Q}$ and $k \in \mathbb{N}_0$.

Note that p -arithmetic sequences, similar to arithmetic progressions are allowed to be sets consisting of a single element (which would be the case when $a = 0$ or $k = 0$ in Definition 3.3). Next we will prove several results regarding p -arithmetic sequences which will be used later in the proof of Theorem 1.3.

Proposition 3.4. *Let p be a prime number.*

- (a) *The intersection of an arithmetic progression with a p -arithmetic sequence is a finite union of p -arithmetic sequences.*
- (b) *Let $a, b \in \mathbb{Q}$ and let $k \in \mathbb{N}_0$. Then the set $\{ap^{kn} + b : n \in \mathbb{N}_0\} \cap \mathbb{N}_0$ is itself a finite union of p -arithmetic sequences.*

Proof. The two parts are actually equivalent; the fact that part (b) is a special case of part (a) is obvious, but also the converse holds. Indeed, letting $a, b, c, d \in \mathbb{Q}$ and $k \in \mathbb{N}_0$, the set of all $cn + d$ which can be written as $ap^{km} + b$ for some $m \in \mathbb{N}_0$ is a p -arithmetic sequence once we know that the set

$$\left\{ \frac{a}{c} \cdot p^{mk} + \frac{b-d}{c} : m \in \mathbb{N}_0 \right\} \cap \mathbb{N}_0$$

is a p -arithmetic sequence. On the other hand, part (b) is a simple exercise using basic properties of congruences. \square

The following proposition is a standard consequence of Siegel's celebrated theorem [Sie29] regarding S -integral points on curves of positive genus.

Proposition 3.5. *Let s be a nonzero algebraic number which is not a root of unity, and let $P(x) \in \bar{\mathbb{Q}}[x]$ be a polynomial of degree d . If there exist infinitely many pairs $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$ such that $P(n) = s^m$, then there exist $a, b \in \bar{\mathbb{Q}}$ such that $P(x) = a(x-b)^d$.*

Proof. We argue by contradiction, and thus assume $P(x)$ has at least two distinct roots (also, note that the case $d = 0$ holds vacuously). We let r_1, \dots, r_ℓ be the distinct roots of $P(x)$ and thus write

$$P(x) = a \cdot \prod_{i=1}^{\ell} (x - r_i)^{e_i} \text{ for some } e_i \in \mathbb{N} \text{ and } a \in \bar{\mathbb{Q}}.$$

We let q be an odd prime number larger than each e_i , and we let $a_1, s_1 \in \bar{\mathbb{Q}}$ such that $a_1^q = a$ and $s_1^q = s$. We let K be a number field containing a_1, s_1 and also each r_i for $i = 1, \dots, \ell$. We let R be the ring of algebraic integers contained in K . We let S be a finite set of (nonzero) prime ideals of R such that all of the following properties hold:

- (i) a_1, s_1 and each r_i are contained in the subring R_S of S -integers in K (i.e., the ring of all elements of K which are integral at all places away from the set S).
- (ii) $r_i - r_j \in R_S^*$ for each $1 \leq i < j \leq \ell$.
- (iii) R_S is a PID.

For each $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$ such that $P(n) = s^m$, conditions (i)-(ii) yield that each ideal $(n - r_i)$ is the q -th power of an ideal in R_S and moreover, using condition (iii) above, we conclude that there exist units $u_i \in R_S^*$ and also elements $z_i \in R_S$ such that $n - r_i = u_i z_i^q$ for each $i = 1, \dots, \ell$. Furthermore, because R_S^* is a finitely generated abelian group and therefore $R_S^*/(R_S^*)^q$ is a finite group, we may and do assume that the units u_i belong to a finite set U of units in the ring R_S . So, by the pigeonhole principle (because there exist infinitely many solutions $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$ for the equation $P(n) = s^m$), there are $u, v \in U$ for which there exist infinitely many $(z, w) \in R_S \times R_S$ such that

$$(9) \quad uz^q - vw^q = r_1 - r_2.$$

Because $q \geq 3$ and $r_1 \neq r_2$, the equation (9) in the variables (z, w) yields a curve of positive genus which cannot contain infinitely many S -integral points, by Siegel's theorem [Sie29]. This concludes our proof that $P(x)$ has only one distinct root. \square

The following fact is an easy consequence of Proposition 3.5.

Corollary 3.6. *Let p be a prime number, let $k \in \mathbb{N}_0$, let $a, b \in \mathbb{Q}$, and let $P \in \mathbb{Q}[x]$ of degree $d \geq 1$. The set T consisting of all $n \in \mathbb{N}_0$ for which there exists $m \in \mathbb{N}_0$ such that $P(n) = b + ap^{mk}$ is a finite union of p -arithmetic sequences.*

Proof. First we note that if T is finite, then the conclusion is obvious; so, from now on, we assume T is infinite. In particular, this yields that both k and a are nonzero.

By Proposition 3.5 we obtain that $P_1(x) := (P(x) - b)/a$ has only one root, which must be thus a rational number (since $P \in \mathbb{Q}[x]$); so, we let $P_1(x) = A(x - c)^d$ for some $c, A \in \mathbb{Q}$. Since there exist infinitely many $n \in \mathbb{N}_0$ such that $P_1(n) = p^{km}$ (actually, even the existence of one such integer n suffices), we conclude that there exists some $\ell \in \mathbb{N}_0$ such that $Ap^{-\ell}$ is the d -th power of a rational number; hence $P_1(x) = p^\ell (ex - f)^d$ for some $e, f \in \mathbb{Q}$ and then the conclusion follows easily (see also part (b) of Proposition 3.4). \square

Proposition 3.7. *Let $\{u_n\}_{n \in \mathbb{N}_0} \subset \mathbb{Z}$ be a linear recurrence sequence, let p be a prime number, let $k \in \mathbb{N}_0$, and let $a, b \in \mathbb{Q}$. Then the set*

$$T = \{n \in \mathbb{N}_0 : u_n = b + ap^{km} \text{ for some } m \in \mathbb{N}_0\}$$

is a finite union of arithmetic progressions along with a finite union of p -arithmetic sequences.

Proof. If $k = 0$ or $a = 0$, then the conclusion follows immediately from Proposition 3.2. So, from now on, we assume that both a and k are nonzero. Also, we assume the set T is infinite (otherwise, the conclusion is obvious).

Because $\{u_n\}_{n \in \mathbb{N}_0}$ is a linear recurrence sequence, then at the expense of replacing $\{u_n\}$ by finitely many linear recurrence sequences (obtained by replacing n by a suitable arithmetic progression $Mn + \ell$, as in Section 3.1), we may assume the sequence $\{u_n\}$ is non-degenerate and for (at least sufficiently large) $n \in \mathbb{N}_0$, we have that

$$(10) \quad u_n = \sum_{i=1}^s P_i(n)r_i^n$$

for some distinct $r_i \in \bar{\mathbb{Q}}^*$ and some nonzero polynomials $P_i(x) \in \bar{\mathbb{Q}}[x]$. Furthermore, if some r_i is a root of unity, then $r_i = 1$; also, if $i \neq j$ then r_i/r_j is not a root of unity. Finally, note that once we know the conclusion of Proposition 3.7 for each sequence $w_n^{(\ell)} = u_{nM+\ell}$ (for $\ell = 0, \dots, M-1$), then we immediately infer the desired conclusion for the original sequence $\{u_n\}_{n \in \mathbb{N}_0}$.

With the above notation and convention for our linear recurrence sequence being non-degenerate and given by the formula (10), if $s = 1$ and $r_1 = 1$, i.e., $u_n = P_1(n)$ for some polynomial $P_1 \in \mathbb{Q}[x]$, then the conclusion follows from Corollary 3.6 (if $\deg(P_1) \geq 1$). Also, note that if $P_1(x)$ is a constant polynomial, then the desired conclusion follows from Proposition 3.2. So, from now on, assume either $s > 1$, or $u_n = P_1(n)r_1^n$ for some non-root of unity r_1 . Since $v_m := b + ap^{km}$ is itself a linear recurrence sequence, and both $\{u_n\}$ and $\{v_m\}$ are non-degenerate linear recurrence sequences which are not of the form $\alpha_0^n Q(n)$ for some root of unity α_0 , and since there exist infinitely many solutions (m, n) for the equation $u_n = v_m$, then [Sch03, Theorem 11.2, p. 209] yields that

$$u_n = b + Q(n)(\pm p^\gamma)^n$$

for some $\gamma \in \mathbb{N}$ and some $Q(x) \in \mathbb{Q}[x]$. We get this conclusion because [Sch03, Theorem 11.2, p. 209] yields that u_n and v_m must be related (see also [Sch03, (11.3), p. 207]) and therefore, u_n has exactly one characteristic root r which is not equal to 1 and furthermore $|r| = p^\gamma$ for some nonzero $\gamma \in \mathbb{Q}$. Since $u_n \in \mathbb{Z}$, then $r = \pm p^\gamma$ and $\gamma \in \mathbb{N}$; so, $u_n = Q_0(n) + Q(n)r^n$. Finally, [Sch03, Theorem 11.2, p. 209] yields that Q_0 must be the constant polynomial equal to b .

Then solving $u_n = v_m$ yields two possibilities: either n is even, or n is odd. Since the latter case follows almost identically as the former case, we focus only on the case n is even. So, we are solving the equation

$$Q(2n)p^{2\gamma n} = ap^{km}$$

and therefore $Q(2n) = ap^{km-2\gamma n}$. If $Q(x)$ is a constant polynomial, then we get that $km - 2\gamma n$ must also be constant and therefore, the set of such $n \in \mathbb{N}_0$ is an arithmetic progression. Now, if $\deg(Q) \geq 1$ then $|Q(2n)| > 1$ for n sufficiently large and therefore, except for finitely many solutions, we must have that $km \geq 2\gamma n$. Then the set of $n \in \mathbb{N}_0$ such that $Q(2n)$ belongs to the the p -arithmetic sequence $\{ap^j\}_{j \in \mathbb{N}_0}$ is itself a finite union of p -arithmetic sequences, as proven in Corollary 3.6. This concludes the proof of Proposition 3.7. \square

Proposition 3.8. *The intersection of two p -arithmetic sequences is a finite union of p -arithmetic sequences.*

Proof. The result is a very simple consequence of Vojta's powerful theorem [Voj96]; however, we can easily prove it directly, as shown in the next few lines.

So, given $a_i, b_i \in \mathbb{Q}$ and $k_i \in \mathbb{N}_0$ for $i = 1, 2$, we look for solutions in $(n_1, n_2) \in \mathbb{N}_0 \times \mathbb{N}_0$ of the equation

$$(11) \quad b_1 + a_1 p^{k_1 n_1} = b_2 + a_2 p^{k_2 n_2}.$$

Now, if some a_i or some k_i equals 0, then the conclusion is immediate. So, from now on, we assume each a_i and each k_i is nonzero. Also, we assume there exist infinitely many solutions to equation (11) since otherwise the conclusion is obvious.

The existence of infinitely many solutions to (11) coupled with [Sch03, Proposition 11.2, p. 209] (or even simpler, using that the p -adic absolute value of $b_1 - b_2$ must be arbitrarily small) yields that $b_1 = b_2$. Then there must be some $\ell \in \mathbb{Z}$ such that $\frac{a_2}{a_1} = p^\ell$. So, equation (11) reads now: $k_1 n_1 = k_2 n_2 + \ell$. The conclusion of Proposition 3.7 follows readily. \square

4. PROOF OF OUR MAIN RESULT

The main ingredient of our proof is the following result.

Theorem 4.1. *Let $(G, +)$ be a finitely generated abelian group, let $y \in G$, and let $\Phi_0 : G \rightarrow G$ be a group homomorphism with the property that there exist $\ell \in \mathbb{N}$ and also there exist $c_0, \dots, c_{\ell-1} \in \mathbb{Z}$ such that*

$$(12) \quad \Phi_0^\ell(x) + c_{\ell-1} \Phi_0^{\ell-1}(x) + \dots + c_1 \Phi_0(x) + c_0 x = 0 \text{ for all } x \in G.$$

Let $\Phi : G \rightarrow G$ be given by $\Phi(x) = y + \Phi_0(x)$ for each $x \in G$, and also let $\alpha \in G$.

- (A) *Let $R \in G$ and let H be a subgroup of G . Then the set S of all $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in (R + H)$ is a union of finitely many arithmetic progressions.*
- (B) *Let p be a prime number, let $k \in \mathbb{N}$, let $R_1, R_2 \in G$, and let*

$$C = \{R_1 + p^{mk} R_2 : m \in \mathbb{N}_0\}.$$

Then the set S of all $n \in \mathbb{N}_0$ such that $\Phi^n(\alpha) \in C$ is a union of finitely many p -arithmetic sequences along with finitely many arithmetic progressions.

Proof. We first prove the following important claim which will be key for both parts of our proposition.

Claim 4.2. There exist linear recurrence sequences $\{u_{i,n}\}_{n \in \mathbb{N}_0} \subset \mathbb{Z}$ for $1 \leq i \leq \ell$ and $\{v_{i,n}\}_{n \in \mathbb{N}_0} \subset \mathbb{Z}$ for $0 \leq i \leq \ell - 1$ such that for each $n \in \mathbb{N}_0$, we have

$$\Phi^n(\alpha) = \sum_{i=1}^{\ell} u_{i,n} \left(\sum_{j=0}^{i-1} \Phi_0^j(y) \right) + \sum_{i=0}^{\ell-1} v_{i,n} \Phi_0^i(\alpha).$$

Proof of Claim 4.2. For each $n \in \mathbb{N}_0$ we have that

$$\Phi^n(\alpha) = \left(\sum_{i=0}^{n-1} \Phi_0^i(y) \right) + \Phi_0^n(\alpha).$$

Due to (12), we get that the sequence of points $\{\Phi_0^n(\alpha)\}_{n \in \mathbb{N}_0}$ satisfies the linear recurrence relation:

$$(13) \quad \Phi_0^{n+\ell}(\alpha) + \sum_{i=0}^{\ell-1} c_i \Phi_0^{n+i}(\alpha) = 0.$$

So, there exist ℓ linear recurrence sequences $\{v_{i,n}\}_{n \in \mathbb{N}_0} \subset \mathbb{Z}$, each one satisfying the linear recurrence formula:

$$(14) \quad v_{i,n+\ell} + \sum_{j=0}^{\ell-1} c_j v_{i,n+j} = 0 \text{ for each } n \in \mathbb{N}_0 \text{ and for each } 0 \leq i \leq \ell - 1,$$

such that

$$(15) \quad \Phi_0^n(\alpha) = \sum_{i=0}^{\ell-1} v_{i,n} \Phi_0^i(\alpha).$$

We let $Q_n := \sum_{i=0}^{n-1} \Phi_0^i(y) \in G$ for $n \geq 1$, and also let $Q_0 := 0$. Because of the linear recurrence formula (12) satisfied by the sequence $\{\Phi_0^n(y)\}_{n \in \mathbb{N}_0}$, we conclude that the sequence $\{Q_n\}_{n \in \mathbb{N}_0}$ satisfies the following linear recurrence sequence:

$$(16) \quad Q_{n+\ell+1} + (c_{\ell-1} - 1)Q_{n+\ell} + \cdots + (c_0 - c_1)Q_{n+1} - c_0 Q_n = 0.$$

The linear recurrence relation (16) yields the existence of the linear recurrence sequences $\{u_{i,n}\}_{n \in \mathbb{N}_0} \subset \mathbb{Z}$ for $1 \leq i \leq \ell$, each of them satisfying the recurrence relation:

$$(17) \quad u_{i,n+\ell+1} + (c_{\ell-1} - 1)u_{i,n+\ell} + \cdots + (c_0 - c_1)u_{i,n+1} - c_0 u_{i,n} = 0$$

such that

$$(18) \quad Q_n = \sum_{i=1}^{\ell} u_{i,n} Q_i.$$

This concludes the proof of Claim 4.2. \square

Now we proceed to proving the two parts of our proposition.

Part (A). Since G is a finitely generated abelian group, we know that G is isomorphic to a direct sum of a finite subgroup G_0 with a subgroup G_1 which is isomorphic to \mathbb{Z}^r for some $r \in \mathbb{N}_0$. We let $\{P_1, \dots, P_r\}$ be a \mathbb{Z} -basis for G_1 . We proceed with the notation from Claim 4.2 and write

$$\Phi^n(\alpha) = \sum_{i=1}^{\ell} u_{i,n} Q_i + \sum_{i=0}^{\ell-1} v_{i,n} \Phi_0^i(\alpha),$$

and then we write each Q_i (for $i = 1, \dots, \ell$) as $Q_{i,0} + \sum_{j=1}^r b_{i,j} P_j$ with $Q_{i,0} \in G_0$ and each $b_{i,j} \in \mathbb{Z}$, and also write each $\Phi_0^i(\alpha)$ (for $i = 0, \dots, \ell - 1$) as $T_{i,0} + \sum_{j=1}^r a_{i,j} P_j$ with $T_{i,0} \in G_0$ and each $a_{i,j} \in \mathbb{Z}$. We also write

$$R = R_0 + \sum_{j=1}^r d_j P_j \text{ with } R_0 \in G_0 \text{ and each } d_j \in \mathbb{Z}.$$

We will write the conditions satisfied by the $u_{i,n}$ and $v_{i,n}$ in order for $\Phi^n(\alpha) \in (R+H)$, or equivalently that $\Phi^n(\alpha) - R \in H$. In order to do this, we let $H_1 = H \cap G_1$, which is also a free abelian finitely generated group, of rank $s \leq r$. Then H is a union of finitely many cosets $U_i + H_1$ with $U_i \in G_0$. Now, for a given $U := U_i$, the condition that $\Phi^n(\alpha) - R \in (U + H_1)$, i.e., that $\Phi^n(\alpha) - R - U \in H_1$ can be written as follows:

$$(19) \quad \sum_{i=1}^{\ell} u_{i,n} Q_{i,0} + \sum_{i=0}^{\ell-1} v_{i,n} T_{i,0} = R_0 + U$$

and

$$(20) \quad \sum_{i=1}^{\ell} u_{i,n} \sum_{j=1}^r b_{i,j} P_j + \sum_{i=0}^{\ell-1} v_{i,n} \sum_{j=1}^r a_{i,j} P_j - \sum_{j=1}^r d_j P_j \in H_1.$$

Now, the set of all $n \in \mathbb{N}_0$ which satisfy condition (19) is a finite union of arithmetic progressions (with the understanding, as always, that a singleton is an arithmetic progression of common difference equal to 0). Indeed, this claim holds since each of the points $Q_{i,0}$, $T_{i,0}$, R_0 and U belong to a finite group, and so they all have finite order bounded by $|G_0|$. Furthermore, it is a standard fact that any linear recurrence sequence of integers is preperiodic modulo any given positive integer (see also the proof of [Ghi08, Claim 3.3]).

So, in order to finish the proof of part (A) of Theorem 4.1, it suffices to prove that the set of all $n \in \mathbb{N}_0$ satisfying condition (20) is also a finite union of arithmetic progressions; clearly, an intersection of two arithmetic progressions is also an arithmetic progression and this would finish our argument for part (A) of our theorem. Collecting coefficients of each P_j for $j = 1, \dots, r$, we get

$$w_{j,n} := \sum_{i=1}^{\ell} b_{i,j} u_{i,n} + \sum_{i=0}^{\ell-1} a_{i,j} v_{i,n} - d_j,$$

and since both $u_{i,n}$ and $v_{i,n}$ are linear recurrence sequences, we conclude that also each $w_{j,n}$ is a linear recurrence sequence. Now, according to [Ghi08, Claim 3.4, Definition 3.5, Subclaim 3.6], the condition (20) is equivalent with a system formed by finitely many equations of the form

$$(21) \quad \sum_{j=1}^r e_j w_{j,n} = 0$$

for some integers e_j , and of the form

$$(22) \quad \sum_{j=1}^r f_j w_{j,n} \equiv 0 \pmod{M},$$

for some other integers f_j and also some $M \in \mathbb{N}$. Since itself, the sequence $\{w_n\}_{n \in \mathbb{N}_0}$ given by $w_n := \sum_{j=1}^r e_j w_{j,n}$ (or respectively $\sum_{j=1}^r f_j w_{j,n}$) is a linear recurrence sequence, we immediately derive that the set of all $n \in \mathbb{N}_0$ satisfying either one of conditions (21) or (22) is a finite union of arithmetic progressions (see also Proposition 3.2).

Part (B). We proceed with the notation from the proof of **Part (A)** for writing $\Phi^n(\alpha) = \sum_{i=1}^{\ell} u_{i,n} Q_i + \sum_{i=0}^{\ell-1} v_{i,n} \Phi_0^i(\alpha)$ in terms of the basis $\{P_1, \dots, P_r\}$ of G_1 . We also write R_1 and R_2 in terms of elements of the finite group G_0 and of the basis $\{P_1, \dots, P_r\}$ of G_1 , as follows:

$$R_i = R_{i,0} + \sum_{j=1}^r d_{i,j} P_j,$$

for some $R_{i,0} \in G_0$ and integers $d_{i,j}$, for $j = 1, \dots, r$ and for $i = 1, 2$. Then $\Phi^n(\alpha) \in C$ if and only if both of the following two conditions are met:

$$(23) \quad \sum_{i=1}^{\ell} u_{i,n} Q_{i,0} + \sum_{i=0}^{\ell-1} v_{i,n} T_{i,0} = R_{1,0} + p^{mk} R_{2,0},$$

and

$$(24) \quad \sum_{i=1}^{\ell} u_{i,n} \sum_{j=1}^r b_{i,j} P_j + \sum_{i=0}^{\ell-1} v_{i,n} \sum_{j=1}^r a_{i,j} P_j = \sum_{j=1}^r (d_{1,j} + p^{mk} d_{2,j}) P_j,$$

for some $m \in \mathbb{N}_0$. Note that for any given $m \in \mathbb{N}_0$, the set of solutions $n \in \mathbb{N}_0$ for the system of equations (23) and (24) is a union of finitely many arithmetic progressions because for fixed m we can easily argue as in part (A). So, from now on, we may assume each integer m for which equations (23) and (24) have a solution $n \in \mathbb{N}_0$ is sufficiently large.

Now, since $R_{2,0}$ is a torsion point, then there exists $s \in \mathbb{N}$ such that for each $e = 0, \dots, s-1$ and for each m in the arithmetic progression $\{e + sj\}$ (for j sufficiently large) the right-hand side of equation (23) is constant, say that it is equal to $R^{(s,e)}$. Replacing m by $e + sm$ in both equations (23) and (24) leads to the following equations:

$$(25) \quad \sum_{i=1}^{\ell} u_{i,n} Q_{i,0} + \sum_{i=0}^{\ell-1} v_{i,n} T_{i,0} = R^{(s,e)}$$

and

$$(26) \quad \sum_{j=1}^r w_{j,n} P_j = \sum_{j=1}^r (d_{1,j} + p^{ke} d_{2,j} \cdot p^{msk}) P_j,$$

where $w_{j,n} := \sum_{i=1}^{\ell} u_{i,n} b_{i,j} + \sum_{i=0}^{\ell-1} v_{i,n} a_{i,j}$ is a linear recurrence sequence of integers for each $j = 1, \dots, r$ because each of the $v_{i,n}$ and $u_{i,n}$ are linear recurrence sequences of integers (and also $b_{i,j}$ and $a_{i,j}$ are integers). We let $b_j := d_{1,j}$ and $a_j := p^{ke} d_{2,j}$ for each $j = 1, \dots, r$.

Since each integer is of the form $sk + e$ for some $e \in \{0, \dots, s-1\}$, it suffices to show that for given e and s , the set of $n \in \mathbb{N}_0$ satisfying simultaneously equations (25) and (26) is a finite union of arithmetic progressions along with a finite union of p -arithmetic sequences.

Because each $Q_{i,0}$ and also each $T_{i,0}$ are torsion elements, while $\{v_{i,n}\}$ and $\{u_{i,n}\}$ are linear recurrence sequences, we conclude that equation (25) is satisfied by integers n which belong to finitely many arithmetic progressions (note that linear recurrence sequences of integers are preperiodic modulo any given integer). Using Proposition 3.4, it suffices to prove that the set of all $n \in \mathbb{N}_0$ satisfying (26) is a finite union of p -arithmetic sequences along with a finite union of arithmetic progressions.

Since equation (26) holds inside a free abelian group whose \mathbb{Z} -basis is given by the P_j 's, then we obtain that (24) is equivalent with the simultaneous solution of the following equations:

$$(27) \quad w_{j,n} = b_j + p^{msk} a_j \text{ for each } j = 1, \dots, r.$$

We have two types of equations of the form (27): either a_j equals 0, or not. If $a_j = 0$, then equation (27) reduces to solving the equation $w_{j,n} = b_j$. If $a_j \neq 0$, then letting $w'_{j,n} := (w_{j,n} - b_j)/a_j$, we get another linear recurrence sequence; moreover, equation (27) yields $w'_{j,n} = p^{skm}$. So, the system of equations (27) splits into finitely many equations of the form

$$(28) \quad w_{j,n} = b_j$$

and also finitely many equations of the form

$$(29) \quad w'_{j,n} = p^{skm}$$

for the same $m \in \mathbb{N}_0$. So, at the expense of re-labelling the linear recurrence sequences $\{w_{j,n}\}$ and $\{w'_{j,n}\}$, we may write the equations (28) and (29) combined as:

$$(30) \quad w'_{1,n} = p^{skm} \text{ for some } m \in \mathbb{N}_0$$

$$(31) \quad w'_{1,n} = w'_{2,n} = \cdots = w'_{i_0,n} \text{ and}$$

$$(32) \quad w_{j,n} = b_j \text{ for } i_0 < j \leq r.$$

The solutions n to equation (30) form finitely many p -arithmetic sequences along with finitely many arithmetic progressions (by Proposition 3.7), while the solutions n to each equation (31) and (32) form finitely many arithmetic progressions (by Proposition 3.2). Another application of Proposition 3.4 along with Proposition 3.8 finishes the proof of Theorem 4.1. \square

Our main result is now a simple consequence of Theorem 4.1.

Proof of Theorem 1.3. Since Φ is a self-map of \mathbb{G}_m^N , then there exists $y \in \mathbb{G}_m^N(K)$ and there exists a group endomorphism Φ_0 of \mathbb{G}_m^N such that $\Phi(x) = y \cdot \Phi_0(x)$ for each $x \in \mathbb{G}_m^N(K)$. We let Γ_0 be the subgroup of $\mathbb{G}_m^N(K)$ spanned by all the coordinates of α and also all coordinates of y , and then we let $\Gamma = \Gamma_0^N \subset \mathbb{G}_m^N(K)$ be its N -th cartesian power. Clearly, Φ_0 induces a group endomorphism of Γ . Furthermore, Φ_0 satisfies (even globally on \mathbb{G}_m^N) an equation such as the one appearing in (12). Indeed, Φ_0 acts on \mathbb{G}_m^N as follows:

$$\Phi_0(x_1, \dots, x_N) = \left(\prod_{i=1}^N x_i^{a_{1,i}}, \dots, \prod_{i=1}^N x_i^{a_{N,i}} \right)$$

for some integers $a_{i,j}$, and therefore, there exist integers c_0, \dots, c_{N-1} such that

$$\Phi_0^N(x) \cdot (\Phi_0^{N-1}(x))^{c_{N-1}} \cdots (\Phi_0(x))^{c_1} \cdot x^{c_0} = 1,$$

for each $x \in \mathbb{G}_m^N(K)$. Applying Corollary 2.3, the intersection $V(K) \cap \Gamma$ is either a finite union of cosets of subgroups of Γ , or a finite union of sets of the form $\left\{ b_i \cdot a_i^{p^{nk}} \right\}_{n \in \mathbb{N}_0}$ (for some $a, b \in \mathbb{G}_m^N(K)$ and some $k \in \mathbb{N}_0$) contained in Γ . At the expense of replacing Γ by a larger finitely generated group, we may even assume that the base points a_i and b_i above are also contained in Γ (and also that Φ_0 restricts to a group endomorphism of Γ). Then the conclusion follows from Theorem 4.1; note also that Proposition 2.4 yields that if S contains an infinite arithmetic progression, then S itself is a finite union of arithmetic progressions. \square

Remark 4.3. It is very difficult to extend the results from the current paper to a proof of Conjecture 1.1 beyond curves V contained in \mathbb{G}_m^N . On one hand, if $V \subset \mathbb{G}_m^N$ is a higher dimensional subvariety, then one deals with products of several F -orbits (see Definition 2.1) and then instead of equation (27), we would have equations of the form:

$$(33) \quad w_n = b + \sum_{i=1}^{\ell} a_i p^{k_i m_i},$$

where $\{w_n\}_{n \in \mathbb{N}_0}$ is a linear recurrence sequence, b and each a_i are rational numbers, while the k_i are nonnegative integers. Finding all $n \in \mathbb{N}_0$ such that the linear recurrence sequence w_n satisfies equation (33) for some $m_i \in \mathbb{N}_0$ is a much more difficult question. For example, a very special case of (33) would be finding all $n \in \mathbb{N}_0$ for which there exist some $m_i \in \mathbb{N}_0$ such that

$$n^d = 1 + \sum_{i=1}^{\ell} 2^{m_i},$$

which is, yet, unsolved when $\ell > 3$ and $d \geq 2$ (see [CZ13]). On the other hand, if we try to solve Conjecture 1.1 in the case of curves V contained in some abelian variety X defined over a finite field \mathbb{F}_q , going through a similar argument as in the proof of Theorem 1.3 we would need to solve equally difficult polynomial-exponential equations of the form

$$(34) \quad Q(n) = v_m,$$

where $Q(x) \in \mathbb{Q}[x]$ and $\{v_m\}$ is a linear recurrence sequence whose characteristic roots are the eigenvalues corresponding to the Frobenius F acting on X . Since these eigenvalues, i.e., the roots of the minimal equation with integer coefficients satisfied by F have all absolute value equal to $q^{\frac{1}{2}}$ (according to the Weil conjectures for abelian varieties over finite fields), the equation (34) is particularly difficult.

Finally, we note that it is unknown whether Moosa-Scanlon result from [MS04] (see also [Ghi08]) extends to non-isotrivial semiabelian varieties X ; hence, in the non-isotrivial case of semiabelian varieties, Conjecture 1.1 is even more difficult since we do not have a complete description of the intersection of a subvariety of X with a finitely generated subgroup of X as in Theorem 2.2.

REFERENCES

- [Bel06] J. P. Bell, *A generalised Skolem-Mahler-Lech theorem for affine varieties*, J. Lond. Math. Soc. (2) **73** (2006), 367–379.
- [BGT10] J. P. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell–Lang problem for étale maps*, Amer. J. Math. **132** (2010), 1655–1675.
- [BGT15] J. P. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell–Lang problem for Noetherian spaces*, Funct. Approx. Comment. Math. **53** (2015), no. 2, 313–328.
- [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.
- [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.
- [Den94] L. Denis, *Géométrie et suites récurrentes*, Bull. Soc. Math. France **122** (1994), 13–27.
- [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.
- [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.
- [GT09] D. Ghioca and T. J. Tucker, *Periodic points, linearizing maps, and the dynamical Mordell–Lang problem*, J. Number Theory **129** (2009), 1392–1403.
- [Hru96] E. Hrushovski, *The Mordell–Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), no. 3, 667–690.
- [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.
- [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.
- [Pet15] C. Petsche, *On the distribution of orbits in affine varieties*, Ergodic Theory Dynam. Systems **35** (2015), no. 7, 2231–2241.
- [Sch03] W. Schmidt, *Linear recurrence sequences*, Diophantine Approximation (Cetraro, Italy, 2000), Lecture Notes in Math. 1819, Springer-Verlag Berlin Heidelberg, 2003, pp. 171–247.
- [Sie29] C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), 41–69. (Reprinted as pp. 209–266 of his Gesammelte Abhandlungen I, Springer, Berlin, 1966.)
- [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.

DRAGOS GHIOCA, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2, CANADA

E-mail address: `dghioca@math.ubc.ca`