MORDELL-LANG AND SKOLEM-MAHLER-LECH THEOREMS FOR ENDOMORPHISMS OF SEMIABELIAN VARIETIES

DRAGOS GHIOCA AND THOMAS J. TUCKER

Abstract. Using the Skolem-Mahler-Lech theorem, we prove a dynamical Mordell-Lang conjecture for semiabelian varieties.

1. Introduction

In 1991, Faltings [Fal94] proved the Mordell-Lang conjecture.

Theorem 1.1 (Faltings)**.** *Let G be an abelian variety defined over the field of complex numbers $\mathbb{C}$. Let $X \subset G$ be a subvariety and $\Gamma \subset G(\mathbb{C})$ a finitely generated subgroup of $G(\mathbb{C})$. Then $X(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ.*

Theorem 1.1 has been generalized to semiabelian varieties G by Vojta (see [Voj96]) and to finite rank subgroups Γ of G by McQuillan (see [McQ95]). Recall that a semiabelian variety (over $\mathbb{C}$) is an extension of an abelian variety by a torus $(\mathbb{G}_m)^k$.

Vojta's result implies that if X is a subvariety of a semiabelian variety G defined over $\mathbb{C}$ and X contains no translate of a positive dimensional algebraic subgroup of G, then for any positive integer n, the intersection of X with the orbit of a point $P \in G(\mathbb{C})$ under the multiplication-by-n-map must be finite. In this paper we describe the intersection of a subvariety of a semiabelian variety G defined over $\mathbb{C}$ with the orbit of a point $P \in G(\mathbb{C})$ under any endomorphism $\phi : G \longrightarrow G$.

Theorem 1.2. *Let G be a semiabelian variety defined over $\mathbb{C}$, and let $V \subset G$ be a subvariety defined over $\mathbb{C}$. Let $\phi \in$ End(G), let $P \in G(\mathbb{C})$, and let $\mathcal{O} := \mathcal{O}_\phi(P)$ be the orbit of P under ϕ. Then $V(\mathbb{C}) \cap \mathcal{O}$ is either empty or a finite union of orbits of the form $\mathcal{O}_{\phi^N}(\phi^\ell(P))$, where $N, \ell \in \mathbb{N}$.*

Prior to Vojta's proof of the semiabelian case of the Mordell-Lang conjecture, Laurent [Lau84] proved the Mordell-Lang conjecture for any power of the multiplicative group. In particular. Laurent's result shows that if $V \subset \mathbb{G}_m^k$ contains no translate of a positive dimensional torus, then V contains finitely many points of the orbit of any point of $\mathbb{A}^k$ under the map $(X_1, \dots, X_k) \mapsto (X_1^{e_1}, \dots, X_k^{e_k})$ (with $e_i \in \mathbb{N}$) on $\mathbb{A}^k$. This led the authors

Date: September 17, 2007.
1991 *Mathematics Subject Classification.* Primary 14G25; Secondary 37F10, 11C08.

conjecture in [GT] that a similar result holds for any polynomial action on the coordinates of the affine plane. This conjecture is the following.

Conjecture 1.3. *Let $F_1,\dots,F_g$ be polynomials in $\mathbb{C}[X]$, let $\mathcal{F}$ be their action coordinatewise on $\mathbb{A}^g$, let $\mathcal{O}_{\mathcal{F}}((a_1,\dots,a_g))$ denote the $\mathcal{F}$-orbit of the point $(a_1,\dots,a_g)\in\mathbb{A}^g(\mathbb{C})$, and let V be a subvariety of $\mathbb{A}^g$. Then V intersects $\mathcal{O}_{\mathcal{F}}((a_1,\dots,a_g))$ in at most a finite union of orbits of the form $\mathcal{O}_{\mathcal{F}^N}(\mathcal{F}^\ell(a_1,\dots,a_g))$, for some non-negative integers N and ℓ.*

Conjecture 1.3 fits into Zhang's far-reaching system of dynamical conjectures [Zha06]. Zhang's conjectures include dynamical analogues of the Manin-Mumford and Bogomolov conjectures for abelian varieties (now theorems of Raynaud [Ray83a, Ray83b], Ullmo [Ull98], and Zhang [Zha98]), as well as a conjecture about the Zariski density of orbits of points under fairly general maps from a projective variety to itself. The latter conjecture is related to our Conjecture 1.3, though neither conjecture contains the other. Conjecture 1.3 has been proved in the case where $g=2$ and V is a line in $\mathbb{A}^2$ (see [GTZ]).

Bell [Bel06] proved Conjecture 1.3 in the case the polynomials F_i are all linear. More precisely, Bell proved that if $\phi:\mathbb{A}^g\to\mathbb{A}^g$ is an automorphism, then for every subvariety $V\subset\mathbb{A}^g$ and any $P\in\mathbb{A}^g$, the set of positive integers k for which $\varphi^k(P)\in V$ is either empty or equal to a finite union of arithmetic progressions. Bell's result is an algebro-geometric generalization of a classical theorem by Skolem [Sko34] (which was later extended by Mahler [Mah35] and Lech [Lec53]). The Skolem-Mahler-Lech theorem says that if $\{u_k\}_{k\in\mathbb{N}}\in\mathbb{C}$ is a linear recurrence sequence, then the set of all $k\in\mathbb{N}$ such that $u_k=0$ is at most a finite union of arithmetic progressions (some of them possibly constant). For a quantitative version of the Skolem-Mahler-Lech theorem, we refer the reader to [ESS02].

The Skolem-Mahler-Lech theorem (see Proposition 3.2) is also instrumental in our proof of Theorem 1.2. For any endomorphism ϕ of a semiabelian variety G defined over $\mathbb{C}$, the ring $\mathbb{Z}[\phi]$ is a finite extension of $\mathbb{Z}$; thus, a cyclic $\mathbb{Z}[\phi]$-module is a finitely generated $\mathbb{Z}$-module. Therefore, for each point $P\in G(\mathbb{C})$, a subvariety V of G intersects the cyclic $\mathbb{Z}[\phi]$-module Γ generated by P in a finite union of cosets of subgroups of Γ. Since

$$V(\mathbb{C})\cap\mathcal{O}_\phi(P)=(V(\mathbb{C})\cap\Gamma)\cap\mathcal{O}_\phi(P),$$

it suffices to describe the intersection of the ϕ-orbit $\mathcal{O}_\phi(P)$ with each coset of a subgroup of Γ, which is done using, among other techniques, also the Skolem-Mahler-Lech theorem. Our argument is similar to the one found in [Ghi] (see also [MS04] for the description of the intersection of subvarieties of a semiabelian variety G defined over a finite field $\mathbb{F}_q$ with $\mathbb{Z}[F]$-submodules of G, where F is the Frobenius on $\mathbb{F}_q$). We note that our methods are not p-adic (as in the case of the classical Skolem-Mahler-Lech theorem), but rather geometric (as in the case of the classical Mordell-Lang conjecture). Thus, they represent a connection of sorts between the Skolem-Mahler-Lech theorem and Mordell-Lang conjecture. It may also be possible to give a purely p-adic analytic proof of Theorem 1.2, using logarithms, following the example of [GT07, GT])

We briefly sketch the plan of our paper. In Section 2 we define the property for a general morphism from a variety into itself to satisfy the "Mordell-Lang condition" (see Definition 2.1), and then we show the connection between the Mordell-Lang condition and our Theorem 1.2, and our Conjecture 1.3. In Section 3 we state the Skolem-Mahler-Lech theorem, while in Section 4 we prove Theorem 1.2.

Notation. Throughout this paper, f^n denotes the n^{th} iterate of the map f. We also use α^n and X^n for the n^{th} power of a constant or of X itself, but this should not cause confusion. We write $\mathbb{N}$ for the set of non-negative integers. An arithmetic progression in $\mathbb{N}$ is a set of the form $\{Nk+\ell : k \in \mathbb{N}\}$ for some $N, \ell \in \mathbb{N}$ (if $N = 0$, then the set consists of only one element $\{\ell\}$). We write $\overline{K}$ for an algebraic closure of the field K.

If $\varphi : V \longrightarrow V$ is a map from a variety to itself and z is a point on V, we define the orbit $\mathcal{O}_\varphi(z)$ of z under φ as

$$\mathcal{O}_\varphi(z) = \{\varphi^k(z) : k \in \mathbb{N}\}.$$

2. An equivalent conjecture

In this section, we present a condition that is equivalent to the conclusions of Theorem 1.2 and of Conjecture 1.3 but has a statement that may seem more familiar.

Definition 2.1. *Let V be a variety over a field L and let $\varphi : V \longrightarrow V$ be a morphism. We say that φ satisfies the* **Mordell-Lang condition** *if for any subvariety W of V and any point z in $V(L)$, there are φ-periodic subvarieties $Y_1, \dots, Y_m$ of W and points $w_1, \dots, w_n$ in W such that*

$$\mathcal{O}_\varphi(z) \cap W = \left(\bigcup_{i=1}^{m} (Y_i \cap \mathcal{O}_\varphi(z))\right) \bigcup \{w_j : 1 \le j \le n\}.$$

Faltings' proof of the Mordell-Lang conjecture and Vojta's extension say the following.

Theorem 2.2. *Let G be a semiabelian variety defined over the field of complex numbers $\mathbb{C}$. Let $X \subset G$ be a subvariety and $\Gamma \subset G(\mathbb{C})$ a finitely generated subgroup of $G(\mathbb{C})$. Then there exist finitely many translates $(y_i + Y_i) \subset X$ of positive dimensional algebraic subgroups $Y_i \subset G$ (for $1 \le i \le m$), and there exist finitely many points $x_j \in X$ (for $1 \le j \le n$), such that*

$$X(\mathbb{C}) \cap \Gamma = \left(\bigcup_{i=1}^{m} (y_i + Y_i) \cap \Gamma\right) \bigcup \{x_j : 1 \le j \le n\}.$$

We also note that according to [Hin88, Lemme 10], if an irreducible subvariety X of a semiabelian variety G is periodic under the multiplication-by-ℓ-map (for $\ell > 1$), then X is a translate of an algebraic subgroup of G.

In this paper we show that any endomorphism of a semiabelian variety over $\mathbb{C}$ satisfies the Mordell-Lang condition. We note that Bell [Bel06] proved that any automorphism of an affine variety also satisfies the Mordell-Lang condition. First we prove an equivalent formulation of the Mordell-Lang condition.

Proposition 2.3. *A morphism $\varphi : V \longrightarrow V$ satisfies the Mordell-Lang condition if and only if for any subvariety W of V and any point $z \in V$, the intersection of W with $\mathcal{O}_\varphi(z)$ is equal to a finite union of orbits of the form $\mathcal{O}_{\varphi^N}(\varphi^\ell(z))$, for some non-negative integers N and ℓ.*

Proof. Note that the proposition is trivial when z is preperiodic under φ. Thus, we assume that z is not preperiodic.

Suppose that

$$\mathcal{O}_\varphi(z) \cap W = \left(\bigcup_{i=1}^{m} (Y_i \cap \mathcal{O}_\varphi(z))\right) \bigcup \{w_j : 1 \le j \le n\}.$$

Then for each Y_i, we let $N := N_i$ be the period of Y_i and for each $r \in \{0, \dots, N-1\}$, we let $\ell := \ell_{i,r}$ be the smallest non-negative integer $\ell \equiv r \pmod{N}$ such that $\varphi^\ell(z) \in Y_i$. For each w_j, we let $N = 0$ and let ℓ be the unique non-negative integer such that $\varphi^\ell(z) = w_j$. Then we see that the intersection of V with $\mathcal{O}_\varphi(z)$ is equal to a finite union of orbits of the form $\mathcal{O}_{\varphi^N}(\varphi^\ell(z))$, for some non-negative integers N and ℓ.

Conversely, suppose that the intersection of V with $\mathcal{O}_\varphi(z)$ is equal to a finite union of orbits of the form $\mathcal{O}_{\varphi^N}(\varphi^\ell(z))$, for some non-negative integers N and ℓ. For each orbit where $N = 0$, we obtain a single point w_j. For each orbit where $N \neq 0$, taking the union of the positive dimensional components of the Zariski closure of the orbit yields a positive dimensional subvariety Y_i of W that is invariant under φ^N. The zero-dimensional components simply give additional points w_j. ∎

Thus, Theorem 1.2 says that any endomorphism ϕ of a semiabelian variety satisfies the Mordell-Lang condition. Furthermore, our Conjecture 1.3 can be reformulated as follows.

Conjecture 2.4. *Let $g \ge 1$, let $F_1, \dots, F_g$ be polynomials in $\mathbb{C}[X]$, and let $\phi : \mathbb{A}^g \longrightarrow \mathbb{A}^g$ be the morphism*

$$\varphi(z_1, \dots, z_g) := (F_1(z_1), \dots, F_g(z_g)).$$

Then φ satisfies the Mordell-Lang condition.

3. The Skolem-Mahler-Lech theorem

In this section we state the Skolem-Mahler-Lech theorem which will be used in our proof of Theorem 1.2. First we need to introduce the basic set-up for *linear recurrence sequences* (see [Eve84] for more details on linear recurrent sequences).

Definition 3.1. *The sequence $\{u_k\}_{k\in\mathbb{N}}$ is a (linear) recurrence sequence, if there exists a positive integer n, and there exist constants $c_1,\dots,c_n$ (with $c_n\neq 0$) such that*

$$u_{k+n}=\sum_{i=1}^{n}c_iu_{k+n-i},\ \text{for each } k\in\mathbb{N}. \tag{3.1}$$

Assume n is the smallest positive integer for which there exist constants $c_1,\dots,c_n$ satisfying (3.1). Every recurrence sequence as above has a *characteristic polynomial*

$$X^n-\sum_{i=1}^{n}c_iX^{n-i},$$

whose roots are called the *characteristic roots* of $\{u_k\}_{k\in\mathbb{N}}$. Note that because $c_n\neq 0$, each characteristic root is nonzero. We let $\{\zeta_i\}_{i=1}^m$ be the distinct characteristic roots of $\{u_k\}_{k\in\mathbb{N}}$. Then there exist (single variable) polynomials $\{f_i\}_{i=1}^m$ such that for each $k\in\mathbb{N}$, we have

$$u_k=\sum_{i=1}^{m}f_i(k)\zeta_i^k. \tag{3.2}$$

If K is an algebraically closed field, and $u_0,\dots,u_{n-1};c_1,\dots,c_n\in K$, then $\zeta_i\in K$ and $f_i\in K[X]$ for each i. Moreover, for *any* given $\zeta_1,\dots,\zeta_m\in K$, and *any* given polynomials $f_1,\dots,f_m\in K[X]$, the sequence $\{u_k\}_{k\in\mathbb{N}}\subset K$ defined by (3.2) satisfies a linear recurrence relation.

The following result is the well-known Skolem-Mahler-Lech theorem (see [ESS02] for a more recent quantitative version).

Proposition 3.2. *Let $m\in\mathbb{N}$, let $\zeta_1,\dots,\zeta_m\in\mathbb{C}^*$, and let $f_1,\dots,f_m\in\mathbb{C}[X]$. Then for every $C\in\mathbb{C}$, the set of all $k\in\mathbb{N}$ such that*

$$\sum_{i=1}^{m}f_i(k)\zeta_i^k=C \tag{3.3}$$

is either empty or a finite union of arithmetic progressions.

4. Semiabelian varieties with an endomorphism

We are ready to prove Theorem 1.2. We begin with some notation and some reductions.

Since every endomorphism of a semiabelian variety is integral over $\mathbb{Z}$, we may let $X^g - \sum_{i=1}^g e_i X^{g-i}$ be the minimal polynomial of ϕ over $\mathbb{Z}$. Then, for each $k \geq 0$, we have

$$\phi^{k+g}(P) = \sum_{i=1}^{g} e_i \phi^{k+g-i}(P). \tag{4.1}$$

If $e_g = 0$, then we let g_1 be the largest index i for which $e_i \neq 0$. Because $\mathcal{O} := \mathcal{O}_\phi(P)$ and $\mathcal{O}_\phi(\phi^{g-g_1}(P))$ differ by finitely many points, it suffices to prove Theorem 1.2 for $\phi^{g-g_1}(P)$ instead of P. Thus, by replacing P with $\phi^{g-g_1}(P)$, we may replace g by g_1 in (4.1). Hence, without loss of generality, we assume that the constant e_g in (4.1) is nonzero.

For each $j \in \{0, \dots, g-1\}$ we define the sequence $\{z_{k,j}\}_{k\geq 0}$ as follows

$$z_{k,j} = 0 \text{ if } 0 \leq k \leq g-1 \text{ and } k \neq j; \tag{4.2}$$

$$z_{j,j} = 1, \text{ and} \tag{4.3}$$

$$z_{k,j} = \sum_{i=1}^{g} c_i z_{k-i,j} \text{ for all } k \geq g. \tag{4.4}$$

Using (4.2) and (4.3) we obtain that

$$\phi^k(P) = \sum_{j=0}^{g-1} z_{k,j}\phi^j(P), \text{ for every } 0 \leq k \leq g-1. \tag{4.5}$$

Using (4.1), (4.4) and (4.5), an easy induction on k shows that

$$\phi^k(P) = \sum_{j=0}^{g-1} z_{k,j}\phi^j(P), \text{ for every } k \geq 0. \tag{4.6}$$

For each j, the sequence $\{z_{k,j}\}_{k\in\mathbb{N}}$ is a linear recurrence sequence; they all have the same characteristic polynomial. Hence there exists $m \in \mathbb{N}$, there exist $\{\gamma_i\}_{1\leq i\leq m} \subset \overline{\mathbb{Q}}$, and there exist $\{f_{j,i}\}_{\substack{0\leq j\leq g-1\\ 1\leq i\leq m}} \subset \overline{\mathbb{Q}}[X]$ such that for every $j \in \{0, \dots, g-1\}$, and for every $k \in \mathbb{N}$, we have

$$z_{k,j} = \sum_{i=1}^{m} f_{j,i}(k)\gamma_i^k. \tag{4.7}$$

The numbers γ_i are the characteristic roots of the recurrence sequences $\{z_{k,j}\}_{k\in\mathbb{N}}$; they are the same for each j.

Since ϕ is integral over $\mathbb{Z}$, the module $\mathbb{Z}[\phi]$ is a finite extension of $\mathbb{Z}$. Therefore, every finitely generated $\mathbb{Z}[\phi]$-module is also a finitely generated $\mathbb{Z}$-module. Let Γ be the cyclic $\mathbb{Z}[\phi]$-module generated by P. Then Γ is a finitely generated $\mathbb{Z}$-module, and so, by Vojta's proof ([Voj96]) of the

Mordell-Lang conjecture for semiabelian varieties, $V(\mathbb{C})\cap\Gamma$ is a finite union of cosets $\{b_i+H_i\}_{i=1}^s$ of subgroups $H_i\subset\Gamma$. Hence

$$V(\mathbb{C})\cap\mathcal{O}=\bigcup_{i=1}^{s}\left((b_i+H_i)\cap\mathcal{O}\right). \tag{4.8}$$

Thus, it suffices to show that for each coset

$$(b+H)\subset\Gamma \tag{4.9}$$

appearing in (4.8), the intersection $(b+H)\cap\mathcal{O}$ is either empty or a finite union of orbits of the form $\mathcal{O}_{\phi^N}(\phi^\ell(P))$, where $N,\ell\in\mathbb{N}$. Let us now fix some notation.

- We write
$$\Gamma=\Gamma_{\mathrm{tor}}\bigoplus\Gamma_1,$$
where Γ_{tor} is a finite torsion group and Γ_1 is a free group of finite rank.
- $\{R_1,\dots,R_n\}$ is a $\mathbb{Z}$-basis for Γ_1.
- For each $j\in\{0,\dots,g-1\}$, we let $T^{(j)}\in\Gamma_{\mathrm{tor}}$ and $Q^{(j)}\in\Gamma_1$ such that $\phi^j(P)=T^{(j)}+Q^{(j)}$.
- For each such j, we let $\{a_{j,i}\}_{1\le i\le n}\subset\mathbb{Z}$ such that
$$Q^{(j)}=\sum_{i=1}^{n}a_{j,i}R_i. \tag{4.10}$$
Then, for each $k\in\mathbb{N}$, we have
$$\phi^k(P)=\left(\sum_{j=0}^{g-1}z_{k,j}T^{(j)}\right)+\left(\sum_{j=0}^{g-1}z_{k,j}\sum_{i=1}^{n}a_{j,i}R_i\right). \tag{4.11}$$
- For b in (4.9), we write $b=b^{(0)}+b^{(1)}$, where $b^{(0)}\in\Gamma_{\mathrm{tor}}$, and $b^{(1)}\in\Gamma_1$.
- We write $H_1:=H\cap\Gamma_1$, where H is as in (4.9).
- For each $h\in\Gamma_{\mathrm{tor}}$, if $(h+\Gamma_1)\cap H$ is not empty, we fix $(h+U_h)\in H$ for some $U_h\in\Gamma_1$.
- For each $h\in\Gamma_{\mathrm{tor}}$, we let
$$\mathcal{O}^{(h)}:=\{\phi^k(P)\in\mathcal{O}:\ \left(-h-b^{(0)}+\phi^k(P)\right)\in\Gamma_1\}.$$

With the above notation, we have

$$\begin{aligned}\mathcal{O}\cap(b+H)&=\bigcup_{h\in\Gamma_{\mathrm{tor}}}\left(\mathcal{O}^{(h)}\cap\left((h+b^{(0)})+(b^{(1)}+U_h+H_1)\right)\right)\\&=\bigcup_{h\in\Gamma_{\mathrm{tor}}}\left((h+b^{(0)})+\left(\left(-h-b^{(0)}+\mathcal{O}^{(h)}\right)\cap(b^{(1)}+U_h+H_1)\right)\right),\end{aligned} \tag{4.12}$$

where $-x+Y:=\{-x+y:\,y\in Y\}$ for every point x, and every subset Y of G. For each $h\in\Gamma_{\mathrm{tor}}$ such that $(h+\Gamma_1)\cap H=\emptyset$ the above intersection is empty (and there is no U_h).

Using (4.11) and (4.12), we conclude that $\mathcal{O}\cap(b+H)$ is a finite union over $h\in\Gamma_{\text{tor}}$ of the points $\phi^k(P)$ corresponding to $k\in\mathbb{N}$ such that

$$\sum_{j=0}^{g-1} z_{k,j}T^{(j)} = h+b^{(0)} \text{ and } \sum_{j=0}^{g-1}\left(z_{k,j}\sum_{i=1}^{n} a_{j,i}R_i\right)\in\left(b^{(1)}+U_h+H_1\right). \tag{4.13}$$

Lemma 4.1. *Let $h\in\Gamma_{\text{tor}}$. The set of $k\in\mathbb{N}$ such that $\sum_{j=0}^{g-1} z_{k,j}T^{(j)}=h$ is either empty or a finite union of arithmetic progressions.*

Proof of Lemma 4.1. Choose $N\in\mathbb{N}$ such that $\Gamma_{\text{tor}}\subset\Gamma[N]$. Then the value of $\sum_{j=0}^{g-1} z_{k,j}T^{(j)}$ is completely determined by the values of the $z_{k,j}$ modulo N. Since there are finitely many g-tuples of integers modulo N, and each $\{z_{k,j}\}_{k\in\mathbb{N}}$ is a linear recurrence sequence of degree g in $\mathbb{Z}$, it follows that each sequence $\{z_{k,j}\}_{k\in\mathbb{N}}$ eventually begins to repeat itself modulo N, i.e. each sequence is preperiodic modulo N. Thus, each value taken by $\sum_{j=0}^{g-1} z_{k,j}T^{(j)}$ is attained for $k\in\mathbb{N}$ living in a finite union of arithmetic progressions. $\square$

We will now prove a more difficult Lemma from which the proof of Theorem 1.2 will follow easily.

Lemma 4.2. *Let $h\in\Gamma_{\text{tor}}$ be fixed such that $(h+\Gamma_1)\cap H$ is not empty. The set of all $k\in\mathbb{N}$ for which*

$$\sum_{j=0}^{g-1}\left(z_{k,j}\sum_{i=1}^{n} a_{j,i}R_i\right)\in\left(b^{(1)}+U_h+H_1\right) \tag{4.14}$$

is either empty or a finite union of arithmetic progressions.

Proof of Lemma 4.2. We first define three classes of subsets of $\mathbb{Z}^n$.

Definition 4.3. *A C-subset of $\mathbb{Z}^n$ is a set $C(d_1,\dots,d_n,D_1,D_2)$, where $d_1,\dots,d_n,D_1,D_2\in\mathbb{Z}$ and $D_2\neq 0$, containing all solutions $(x_1,\dots,x_n)\in\mathbb{Z}^n$ of $\sum_{i=1}^n d_ix_i\equiv D_1 \pmod{D_2}$.*

An L-subset of $\mathbb{Z}^n$ is a set $L(d_1,\dots,d_n,D)$, where $d_1,\dots,d_n,D\in\mathbb{Z}$, containing all solutions $(x_1,\dots,x_n)\in\mathbb{Z}^n$ of $\sum_{i=1}^n d_ix_i=D$.

A CL-subset of $\mathbb{Z}^n$ is either a C-subset or an L-subset of $\mathbb{Z}^n$.

The C-subsets may be thought of as satisfying congruence relations, while the L-subsets satisfy linear conditions.

Claim 4.4. *There exist CL-subsets $S_1,\dots,S_n$ of $\mathbb{Z}^n$ such that a point $R:=\sum_{i=1}^n c^{(i)}R_i$ lies in $U_h+b^{(1)}+H_1$ if and only if*

$$(c^{(1)},\dots,c^{(n)})\in\bigcap_{i=1}^n S_i.$$

Proof of Claim 4.4. Because $H_1\subset\Gamma_1$ and Γ_1 is a free $\mathbb{Z}$-module with basis $\{R_1,\dots,R_n\}$, we can find (after a possible relabeling of $R_1,\dots,R_n$) a $\mathbb{Z}$-basis $Q_1,\dots,Q_\ell$ (with $1\le\ell\le n$) of H_1 of the following form:

$$Q_1=\beta_1^{(i_1)}R_{i_1}+\cdots+\beta_1^{(n)}R_n;$$

$$Q_2 = \beta_2^{(i_2)} R_{i_2} + \cdots + \beta_2^{(n)} R_n;$$

and in general

$$Q_j = \beta_j^{(i_j)} R_{i_j} + \cdots + \beta_j^{(n)} R_n \tag{4.15}$$

for each $j \le \ell$, where

$$1 \le i_1 < i_2 < \cdots < i_\ell \le n$$

and all $\beta_j^{(i)} \in \mathbb{Z}$. We also assume $\beta_j^{(i_j)} \ne 0$ for every $j \in \{1, \dots, \ell\}$.

Let $b_{1,1}, \dots, b_{1,n} \in \mathbb{Z}$ such that $b^{(1)} + U_h = \sum_{j=1}^n b_{1,j} R_j$. Then $R \in (b^{(1)} + U_h + H_1)$ if and only if there exist integers $k_1, \dots, k_\ell$ such that

$$R = b^{(1)} + U_h + \sum_{i=1}^{\ell} k_i Q_i. \tag{4.16}$$

Using the expressions for the Q_i (in (4.15)), $(b^{(1)} + U_h)$, and R in terms of the $\mathbb{Z}$-basis $\{R_1, \dots, R_n\}$ of Γ_1, we obtain the following relations for the coefficients $c^{(j)}$:

$$c^{(j)} = b_{1,j} \text{ for every } 1 \le j < i_1; \tag{4.17}$$

$$c^{(j)} = b_{1,j} + k_1 \beta_1^{(j)} \text{ for every } i_1 \le j < i_2; \tag{4.18}$$

$$c^{(j)} = b_{1,j} + k_1 \beta_1^{(j)} + k_2 \beta_2^{(j)} \text{ for every } i_2 \le j < i_3 \tag{4.19}$$

and so on, until

$$c^{(n)} = b_{1,n} + \sum_{i=1}^{\ell} k_i \beta_i^{(n)}. \tag{4.20}$$

We interpret the above relations as follows: the numbers $c^{(1)}, \dots, c^{(n)}$ are the unknowns, while the numbers $k_1, \dots, k_\ell$ are integer parameters, and all $b_{1,i}$ and $\beta_j^{(i)}$ are integer constants. We will show, by eliminating the parameters k_i, that the unknowns $c^{(j)}$ must satisfy ℓ linear congruences and $(n - \ell)$ linear equations with coefficients involving only the $b_{1,i}$ and the $\beta_j^{(i)}$. Each such equation will generate a CL-set.

We begin by expressing equation (4.18) for $j = i_1$ as a linear congruence modulo $\beta_1^{(i_1)}$ and obtain

$$c^{(i_1)} \equiv b_{1,i_1} \left(\bmod \beta_1^{(i_1)}\right). \tag{4.21}$$

Equation (4.18) also gives us $k_1 = \frac{c^{(i_1)} - b_{1,i_1}}{\beta_1^{(i_1)}}$. Substituting this formula for k_1 into (4.18) for each $i_1 < j < i_2$, we obtain

$$c^{(j)} = b_{1,j} + \frac{c^{(i_1)} - b_{1,i_1}}{\beta_1^{(i_1)}} \beta_1^{(j)} \text{ for every } i_1 < j < i_2. \tag{4.22}$$

We then express (4.19) for $j = i_2$ as a linear congruence modulo $\beta_2^{(i_2)}$ (also using the expression for k_1 computed above). We obtain

$$c^{(i_2)} \equiv b_{1,i_2} + \frac{c^{(i_1)} - b_{1,i_1}}{\beta_1^{(i_1)}}\beta_1^{(i_2)} \left(\bmod \beta_2^{(i_2)}\right). \tag{4.23}$$

Next we solve for k_2 using (4.19) for $j = i_2$ (along with our formula above for k_1) and obtain

$$k_2 = \frac{c^{(i_2)} - b_{1,i_2} - \frac{c^{(i_1)} - b_{1,i_1}}{\beta_1^{(i_1)}}\beta_1^{(i_2)}}{\beta_2^{(i_2)}}.$$

Then we substitute this formula for k_2 in (4.19) for $i_2 < j < i_3$ and obtain

$$c^{(j)} = b_{1,j} + \frac{c^{(i_1)} - b_{1,i_1}}{\beta_1^{(i_1)}} \cdot \beta_1^{(j)} + \frac{c^{(i_2)} - b_{1,i_2} - \frac{c^{(i_1)} - b_{1,i_1}}{\beta_1^{(i_1)}}\beta_1^{(i_2)}}{\beta_2^{(i_2)}} \cdot \beta_2^{(j)}. \tag{4.24}$$

Continuing onward in this manner, we express $c^{(n)}$ in terms of the integers $b_{1,i_1}, \dots, b_{1,i_\ell}, b_{1,n}$, $c^{(i_1)}, \dots, c^{(i_\ell)}$, and $\{\beta_j^{(i)}\}_{j,i}$.

We observe that all of the above congruences and linear equations can be written as linear congruences or linear equations over $\mathbb{Z}$ (after clearing the denominators). For example, the congruence equation (4.23) can be written as the following linear congruence over $\mathbb{Z}$:

$$\beta_1^{(i_1)} \cdot c^{(i_2)} \equiv \beta_1^{(i_1)} b_{1,i_2} + \left(c^{(i_1)} - b_{1,i_1}\right)\beta_1^{(i_2)} \left(\bmod \beta_1^{(i_1)} \cdot \beta_2^{(i_2)}\right).$$

Hence all the above conditions that must be satisfied by $c^{(j)}$ for which

$$\sum_{j=1}^{n} c^{(j)} R_j \in (b^{(1)} + U_h + H_1)$$

are either linear equations over $\mathbb{Z}$ (giving rise to L-subsets) or linear congruences over $\mathbb{Z}$ (giving rise to C-subsets). There are precisely ℓ congruences (corresponding to the ℓ degrees of freedom introduced by the parameters k_i) and $(n - \ell)$ linear equations. This concludes the proof of Claim 4.4. □

We will now show that for each S_i that appears in Claim 4.4, there exists at most finitely many arithmetic progressions $W_j^{(i)} \subset \mathbb{N}$ such that $k \in \bigcup_j W_j^{(i)}$ if and only if $(c^{(1)}, \dots, c^{(n)}) \in S_i$, where

$$\sum_{i=1}^{n} c^{(i)} R_i := \sum_{j=0}^{g-1} \left(z_{k,j} \sum_{i=1}^{n} a_{j,i} R_i\right).$$

This will show that there exists at most a finite number of arithmetic progressions

$$\widetilde{W} := \bigcap_{i=1}^{n} \left(\bigcup_j W_j^{(i)} \right) \subset \mathbb{N}$$

such that $k \in \widetilde{W}$ if and only if

$$\sum_{j=0}^{g-1} \big(z_{k,j} \sum_{i=1}^{n} a_{j,i}\big) R_i \in \Big(b^{(1)} + U_h + H_1\Big). \tag{4.25}$$

Claim 4.5. *Let $C := C(d_1, \dots, d_n, D_1, D_2)$ be a* C*-subset of $\mathbb{Z}^n$. There exists at most a finite number of arithmetic progressions $W_j \subset \mathbb{N}$ such that $k \in \bigcup_j W_j$ if and only if $(c^{(1)}, \dots, c^{(n)}) \in C$, where*

$$\sum_{i=1}^{n} c^{(i)} R_i := \sum_{j=0}^{g-1} \big(z_{k,j} \sum_{i=1}^{n} a_{j,i} R_i\big). \tag{4.26}$$

Proof of Claim 4.5. Using (4.26), we conclude that for every $1 \le i \le n$, we have

$$c^{(i)} = \sum_{j=0}^{g-1} a_{j,i} z_{k,j}. \tag{4.27}$$

Hence, the congruence equation $\sum_{i=1}^{n} d_i c^{(i)} \equiv D_1 \pmod{D_2}$ yields the congruence

$$\sum_{j=0}^{g-1} h_j z_{k,j} \equiv D_1 \pmod{D_2} \tag{4.28}$$

for integers $h_j := \sum_{i=1}^{n} d_i a_{j,i}$, for each $0 \le j \le g-1$ (we recall that all $a_{j,i} \in \mathbb{Z}$). As noted in the proof of Lemma 4.1, recursively defined sequences over $\mathbb{Z}$, such as $\{z_{k,j}\}_{k \in \mathbb{N}}$, are preperiodic modulo any nonzero integer (hence, they are preperiodic modulo D_2). Therefore the set of all solutions $k \in \mathbb{N}$ to (4.28) is at most a finite union $\bigcup_j W_j$ of arithmetic progressions in $\mathbb{N}$. □

Claim 4.6. *Let $L := L(d_1, \dots, d_n, D)$ be an* L*-subset of $\mathbb{Z}^n$. There exist at most finitely many arithmetic progressions $W_j \subset \mathbb{N}$ such that $k \in \bigcup_j W_j$ if and only if $(c^{(1)}, \dots, c^{(n)}) \in L$, where*

$$\sum_{i=1}^{n} c^{(i)} R_i := \sum_{j=0}^{g-1} \big(z_{k,j} \sum_{i=1}^{n} a_{j,i} R_i\big). \tag{4.29}$$

Proof of Claim 4.6. Using (4.29) and (4.7), we conclude that for every $1 \le i \le n$, we have

$$c^{(i)} = \sum_{j=0}^{g-1} a_{j,i} \sum_{\ell=1}^{m} f_{j,\ell}(k) \gamma_\ell^k. \tag{4.30}$$

The linear equation $\sum_{i=1}^n d_i c^{(i)} = D$ yields the following equation (after collecting the coefficients of γ_ℓ^k for each $1 \le \ell \le m$):

$$\sum_{\ell=1}^{m} f_\ell(k)\gamma_\ell^k = D, \tag{4.31}$$

where $f_\ell := \sum_{j=0}^{g-1}\sum_{i=1}^n d_i a_{j,i}\cdot f_{j,\ell} \in \overline{\mathbb{Q}}[X]$ for each $\ell \in \{1,\dots,m\}$. Using Proposition 3.2, the set of all $k \in \mathbb{N}$ satisfying (4.31) is at most a finite union of arithmetic progressions, as desired. □

Since the intersection of two arithmetic progressions in $\mathbb{N}$ is another arithmetic progression (or the empty set), Claims 4.5 and 4.6 finish the proof of Lemma 4.2. □

We are now ready to complete the proof of Theorem 1.2.

Proof of Theorem 1.2. It follows from Lemmas 4.1 and 4.2, that for each fixed $h \in \Gamma_{\text{tor}}$, there is at most a finite union W_h of arithmetic progressions in $\mathbb{N}$ such that $k \in \mathbb{N}$ satisfies the equations

$$\sum_{j=0}^{g-1} z_{k,j}T^{(j)} = h + b^{(0)} \quad \text{and} \tag{4.32}$$

$$\sum_{j=0}^{g-1}\left(z_{k,j}\sum_{i=1}^{n} a_{j,i}R_i\right) \in \left(b^{(1)} + U_h + H_1\right) \tag{4.33}$$

if and only if $k \in W_h$. Using (4.12), (4.13), and that Γ_{tor} is finite, we conclude that the set of all $k \in \mathbb{N}$ for which $\phi^k(P) \in (b+H)$ is either empty or a finite union of arithmetic progressions. □

References

[Bel06] J. P. Bell, *A generalised Skolem-Mahler-Lech theorem for affine varieties*, J. London Math. Soc. (2) **73** (2006), no. 2, 367–379.

[ESS02] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2) **155** (2002), no. 3, 807–836.

[Eve84] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio. Math. **53** (1984), no. 2, 225–244.

[Fal94] G. Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., no. 15, Academic Press, San Diego, CA, 1994, pp. 175–182.

[Ghi] D. Ghioca, *The isotrivial case in the Mordell-Lang theorem*, to appear in Tran. Amer. Soc., 2006, available online at `http://www.cs.uleth.ca/~ghioca/papers/papers.html`, 18 pages.

[GT] D. Ghioca and T. J. Tucker, *p-adic logarithms for polynomial dynamics*, submitted for publication, 2007, available online at `http://www.arxiv.org/pdf/math/0705.4047`, 11 pages.

[GT07] D. Ghioca and T. J. Tucker, *A dynamical version of the Mordell-Lang theorem for the additive group*, submitted for publication, available online at `http://www.arxiv.org/pdf/0704.1333`, 13 pages, 2007.

[GTZ] D. Ghioca, T. J. Tucker, and M. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, submitted for publication, 2007, available online at `http://arxiv.org/pdf/0705.1954`, 19 pages.

[Hin88] M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), no. 3, 575–603.

[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.

[Mah35] K. Mahler, *Eine arithmetische Eigenshaft der Taylor-Koeffizienten rationaler Funktionen*, Proc. Kon. Nederlandsche Akad. v. Wetenschappen **38** (1935), 50–60.

[McQ95] M. McQuillan, *Division points on semi-abelian varieties*, Invent. Math. **120** (1995), no. 1, 143–159.

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

[Ray83a] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), no. 1, 207–233.

[Ray83b] ______, *Sous-variétés d'une variété abélienne et points de torsion*, Arithmetic and geometry, vol. I, Progr. Math., vol. 35, Birkhäuser, Boston, MA, 1983, pp. 327–352.

[Sko34] T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, C. r. 8 congr. scand. à Stockholm (1934), 163–188.

[Ull98] E. Ullmo, *Positivité et discrétion des points algébriques des courbes*, Ann. of Math. (2) **147** (1998), no. 1, 167–179.

[Voj96] P. Vojta, *Integral points on subvarieties of semiabelian varieties. I*, Invent. Math. **126** (1996), no. 1, 133–181.

[Zha98] S. Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), no. 1, 159–165.

[Zha06] S. Zhang, *Distributions in Algebraic Dynamics*, Survey in Differential Geometry, vol. 10, International Press, 2006, pp. 381–430.

Dragos Ghioca, Department of Mathematics & Computer Science, University of Lethbridge, 4401 University Drive, Lethbridge, Alberta T1K 3M4

E-mail address: `ghioca@cs.uleth.ca`

Thomas Tucker, Department of Mathematics, Hylan Building, University of Rochester, Rochester, NY 14627

E-mail address: `ttucker@math.rochester.edu`