Dragos GHIOCA, Thomas TUCKER et Michael E. ZIEVE

The Mordell–Lang question for endomorphisms of semiabelian varieties

The Mordell–Lang question for endomorphisms of semiabelian varieties

par Dragos GHIOCA, Thomas TUCKER et Michael E. ZIEVE

RÉSUMÉ. La conjecture de Mordell-Lang décrit l'intersection d'un sous-groupe de type fini avec une variété fermée d'une variété semi-abélienne. De façon équivalente, cette conjecture décrit l'intersection des sous-variétés fermées avec l'ensemble des images de l'origine sous un semigroupe de translations de type fini. Nous étudions la question analogue dans laquelle les translations sont remplacées par les endomorphismes d'un groupe algébrique (et l'origine est remplacée par un autre point). Nous montrons qui la conclusion de la conjecture de Mordell-Lang reste vraie dans cette situation si, ou bien, (1) la variété semi-abélienne est simple, ou, (2) la variété semi-abélienne est A^2, où A est une variété semi-abéliennne de dimension 1, ou (3) la sous-variété est une sous-variété semi-abéliennne de dimension 1, ou enfin, (4) la matrice jacobienne à l'origine de chaque endomorphisme est diagonalisable. Nous donnons aussi des exemples qui montrent que la conclusion est fausse si nous affaiblissons n'importe laquelle de ces hypothéses.

ABSTRACT. The Mordell–Lang conjecture describes the intersection of a finitely generated subgroup with a closed subvariety of a semiabelian variety. Equivalently, this conjecture describes the intersection of closed subvarieties with the set of images of the origin under a finitely generated semigroup of translations. We study the analogous question in which the translations are replaced by algebraic group endomorphisms (and the origin is replaced by another point). We show that the conclusion of the Mordell–Lang conjecture remains true in this setting if either (1) the semiabelian variety is simple, (2) the semiabelian variety is A^2, where A is a one-dimensional semiabelian variety, (3) the subvariety is a connected one-dimensional algebraic subgroup, or (4) each endomorphism has diagonalizable Jacobian at the origin. We also give examples showing that the conclusion fails if we make slight modifications to any of these hypotheses.

1. Introduction

Lang's generalization of the Mordell conjecture describes the intersection of certain subgroups and subvarieties of algebraic groups. Specifically, this conjecture addresses *semiabelian varieties*, which are the connected algebraic groups G admitting an exact sequence

$$1 \to \mathbb{G}_m^k \to G \to A \to 1$$

with A an abelian variety and $\mathbb{G}_m$ the multiplicative (algebraic) group. The Mordell–Lang conjecture, proved by Faltings [6] for abelian varieties and by Vojta [18] in general, is as follows:

Theorem 1.1. *Let G be a semiabelian variety defined over $\mathbb{C}$. Let V be a closed subvariety of G, and let Γ be a finitely generated subgroup of $G(\mathbb{C})$. Then $V(\mathbb{C}) \cap \Gamma$ is the union of finitely many cosets of subgroups of Γ.*

McQuillan [15] extended Vojta's result to the case of finite rank subgroups $\Gamma \subset G(\mathbb{C})$, i.e. when $\dim_{\mathbb{Q}} \Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$ is finite.

We can view Theorem 1.1 as a dynamical assertion by writing Γ as the set of images of the origin under translations by elements of Γ. We will study the analogous problem in which the translation maps are replaced by more general endomorphisms of G, and the origin is replaced by an arbitrary point of $G(\mathbb{C})$. In this setting, the analogue of Γ is not generally a group, so we must reformulate the conclusion of Theorem 1.1, as follows:

Question 1.2. *Let G be a semiabelian variety defined over $\mathbb{C}$, let $\Phi_1, \ldots, \Phi_r$ be commuting endomorphisms of G, let V be a closed subvariety of G, and let $\alpha \in G(\mathbb{C})$. Let E be the set of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V(\mathbb{C})$. Is E the union of finitely many sets of the form $u + (\mathbb{N}^r \cap H)$ with $u \in \mathbb{N}^r$ and H a subgroup of $\mathbb{Z}^r$?*

Theorem 1.1 implies that the answer is 'yes' if each Φ_i is a translation (even if $\alpha \neq 0$); conversely, it is not difficult to deduce Theorem 1.1 as a consequence of Question 1.2 in case the Φ_i are translations. The crucial fact here is that the group of points on a semiabelian variety is commutative [11, Lemma 4]. On a related note, one could consider Question 1.2 for noncommuting endomorphisms, but we know of almost no results in this setting.

Each endomorphism of a semiabelian variety is the composition of a translation and an algebraic group endomorphism [10, Thm. 2]. Question 1.2 generally has a negative answer if the Φ_i's include both translations and algebraic group endomorphisms. For instance, let P_0 be a nontorsion point on a semiabelian variety G_0, and let V be the diagonal in $G := G_0^2$; for

$$\Phi_1 \colon (x, y) \mapsto (x + P_0, y) \quad \text{and} \quad \Phi_2 \colon (x, y) \mapsto (x, 2y),$$

if $\alpha = (0, P_0)$ then $E = \{(2^k, k) : k \in \mathbb{N}_0\}$ does not have the desired form. However, we will show that Question 1.2 often has an affirmative answer when every Φ_i is an algebraic group endomorphism.

Theorem 1.3. *Let G be a semiabelian variety defined over $\mathbb{C}$, let $\alpha \in G(\mathbb{C})$, let $V \subset G$ be a closed subvariety, and let $\Phi_1, \ldots, \Phi_r$ be commuting algebraic group endomorphisms of G. Assume that either*

(a) *The Jacobian at 0 of each endomorphism Φ_i is diagonalizable; or*
(b) *V is a connected algebraic subgroup of G of dimension one; or*
(c) *$G = A^j$ for $0 \le j \le 2$, where A is a one-dimensional semiabelian variety.*

Then the set E of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $\Phi_1^{n_1} \ldots \Phi_r^{n_r}(\alpha) \in V(\mathbb{C})$ is the union of finitely many sets of the form $u + (\mathbb{N}^r \cap H)$ with $u \in \mathbb{N}^r$ and H a subgroup of $\mathbb{Z}^r$.

It is immediate to see that if condition (a) holds in Theorem 1.3, then the Jacobian at 0 of *each* endomorphism of the semigroup S generated by the Φ_i's is diagonalizable.

The first two authors showed in [7] that the conclusion of Theorem 1.3 holds when $r = 1$, even if one does not assume (a), (b), or (c). However, in Section 6 we will give examples with $r = 2$ and $G = \mathbb{G}_m^3$ where the conclusion of Theorem 1.3 does not hold. Our examples lie just outside the territory covered by Theorem 1.3, as V is a coset of a one-dimensional algebraic subgroup of G in the first example, and V is a two-dimensional algebraic subgroup of G in the second example.

In our previous paper [9] we discussed a more general version of Question 1.2 involving endomorphisms of an arbitrary variety.

Question 1.4. *Let X be any quasiprojective variety defined over $\mathbb{C}$, let $\Phi_1, \ldots, \Phi_r$ be commuting endomorphisms of X, let V be a closed subvariety of G, and let $\alpha \in X(\mathbb{C})$. Let E be the set of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V(\mathbb{C})$. Is E the union of finitely many sets of the form $u + (\mathbb{N}^r \cap H)$ with $u \in \mathbb{N}^r$ and H a subgroup of $\mathbb{Z}^r$?*

The only known instances where Question 1.4 has an affirmative answer are the results of the present paper, the results of our previous paper [9], the Mordell–Lang conjecture itself, and various cases with $r = 1$ [17, 14, 13, 5, 1, 8, 3, 7, 2].

Here is a rough sketch of our proof for Theorem 1.3. At the expense of replacing V by the Zariski closure of the intersection $V(\mathbb{C}) \cap \mathcal{O}_S(\alpha)$, we may assume that $\mathcal{O}_S(\alpha)$ is Zariski dense in V. In particular, letting Γ be the finitely generated subgroup of $G(\mathbb{C})$ generated by $\mathcal{O}_S(\alpha)$, we obtain that $V(\mathbb{C}) \cap \Gamma$ is Zariski dense in V. So, assuming V is irreducible, Theorem 1.1 yields that V is a coset of an algebraic subgroup of G. We may choose a suitable prime number p and then find a suitable model of the semiabelian

variety G over $\mathbb{Z}_p$; finally, using the p-adic exponential map on G, we reduce the problem to a question of linear algebra inside $\mathbb{C}_p^g$ (where $\dim(G) = g$). Given finitely many commuting matrices $J_i \in M_{g,g}(\mathbb{C}_p)$ (for $i = 1, \ldots, r$), given $u_0, v_0 \in \mathbb{C}_p^g$, and given a linear subvariety $\mathcal{V} \subset \mathbb{C}_p^g$, we need to describe the set E of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ such that $J_1^{n_1} \cdots J_r^{n_r}(u_0) \in (v_0 + \mathcal{V})$. We show that E has the description from the conclusion of Theorem 1.3 if either (a) each J_i is diagonalizable, or (b) $\dim(\mathcal{V}) = 1$ and v_0 is the zero vector, or (c) $g = 2$ and the matrices J_i are all defined over the ring of integers in a quadratic imaginary field.

The contents of this paper are as follows. In the next section we prove some basic results regarding semigroups of $\mathbb{N}^r$ which are used throughout our proofs. As a consequence of our results from Section 2, we prove in Proposition 2.11 that Question 1.4 has a positive answer in greater generality assuming $\dim(V) = 0$. Then in Section 3 we prove several preliminary results towards proving Theorem 1.3, while in Section 4 we reduce the proof of our results to propositions on linear algebra by using suitable p-adic parametrizations. Then in Section 5 we prove Theorem 1.3. Finally, in Section 6 we provide counterexamples to our theorem if we relax its hypothesis.

Notation. In this paper, each subvariety is closed, and each semigroup contains an identity element. We also denote by $\mathbb{N}$ the set of all nonnegative integers.

For any algebraic group G, we denote by $\mathrm{End}(G)$ the set of all algebraic group endomorphisms of G.

For any set T, for any set S of maps $\Psi \colon T \to T$, and for any $\alpha \in T$, we let $\mathcal{O}_S(\alpha) := \{\Psi(\alpha) : \Psi \in S\}$ be the S-orbit of α.

We will use the following definition: if Φ is an endomorphism of the quasiprojective variety X, and if V is a subvariety of X, then we say that V is *preperiodic* under Φ if there exist $k, \ell \in \mathbb{N}$ with $k < \ell$ such that $\Phi^k(V) = \Phi^\ell(V)$. If we may take $k = 0$ in the above definition, then we say that V is *periodic* under Φ.

2. Semigroups of $\mathbb{N}^r$

In this section we provide basic results regarding subsets of $\mathbb{N}^r$. We start with a definition.

Definition 2.1. *We denote by $\mathcal{C}$ the class of all sets of the form*

$$\bigcup_{i=1}^{\ell} \left(\gamma_i + H_i \cap \mathbb{N}^r\right),$$

for some nonnegative integers ℓ and r, and for some $\gamma_i \in \mathbb{N}^r$, and for some subgroups $H_i \subset \mathbb{Z}^r$.

In our proofs we will use the following order relation on $\mathbb{N}^r$.

Definition 2.2. *We define the order $\prec_r$ on $\mathbb{N}^r$ as follows:*

$$(\beta_1, \ldots, \beta_r) \prec_r (\gamma_1, \ldots, \gamma_r)$$

if and only if $\beta_i \le \gamma_i$ for all $i = 1, \ldots, r$. Equivalently, $\beta \prec_r \gamma$ as elements of $\mathbb{Z}^r$ if and only if $\gamma - \beta \in \mathbb{N}^r$. When it is clear in the context, we will drop the index r from $\prec_r$ and simply denote it by $\prec$.

Additionally, for each subset $S \subset \mathbb{N}^r$, we call $\gamma \in S$ a minimal element (with respect to the above ordering) if there exists no $\beta \in S \setminus \{\gamma\}$ such that $\beta \prec \gamma$.

Our first result will be used many times throughout our paper, and it is an easy consequence of the order relation $\prec_r$ on $\mathbb{N}^r$.

Proposition 2.3. *Any subset $S \subset \mathbb{N}^r$ has at most finitely many minimal elements with respect to $\prec_r$.*

Proof. Assume S is nonempty (otherwise the statement is vacuously true). We prove the result by induction on r. The case $r = 1$ is obvious.

Now, assume the result is proved for $r \le k$ and we prove it for $r = k+1$ (for some $k \in \mathbb{N}$). Let π be the natural projection of $\mathbb{N}^{k+1}$ on its last k coordinates, and let $S_1 = \pi(S)$. Let M_1 be the set of minimal elements for S_1 with respect to the ordering $\prec_k$ of $\mathbb{N}^k$ defined on the last k coordinates of $\mathbb{N}^{k+1}$; according to the induction hypothesis, M_1 is a finite set. For each $\overline{\gamma_1} \in M_1$, we let $\overline{\gamma} \in S$ be the minimal element of $\pi^{-1}(\overline{\gamma_1}) \cap S$ with respect to the ordering $\prec_{k+1}$ on $\mathbb{N}^{k+1}$. Obviously, $\overline{\gamma} = (\gamma_1, \overline{\gamma_1}) \in \mathbb{N} \times \mathbb{N}^k$ with $\gamma_1 \in \mathbb{N}$ minimal such that $\pi(\overline{\gamma}) = \overline{\gamma_1}$; we let M_0 be the finite set of all these $\overline{\gamma}$.

Let ℓ be the maximum of all $\gamma_1 \in \mathbb{N}$ such that there exists $\overline{\gamma_1} \in M_1$ for which $(\gamma_1, \overline{\gamma_1}) \in M_0$. Then for each $i = 0, \ldots, \ell - 1$, we let $S_{1,i} = \pi\left(S \cap \left(\{i\} \times \mathbb{N}^k\right)\right)$. Again using the induction hypothesis, there exists at most a finite set $M_{1,i}$ of minimal elements of $S_{1,i}$ with respect to $\prec_k$. We let $M_{0,i}$ be the set (possibly empty) given by $M_{0,i} := \left(\{i\} \times \mathbb{N}^k\right) \cap \pi^{-1}(M_{1,i})$, and we let $M := M_0 \bigcup \left(\bigcup_{i=0}^{\ell-1} M_{0,i}\right)$. Then M is a finite set, and we claim that it contains all minimal elements of S. Indeed, if $(\beta_1, \ldots, \beta_{k+1}) \in S \setminus M$ is a minimal element with respect to $\prec_{k+1}$, then there are two possibilities.

Case 1. $(\beta_2, \ldots, \beta_{k+1}) \in M_1$, i.e. $(\beta_2, \ldots, \beta_{k+1})$ is a minimal element of S_1.

In this case, since $(\beta_1, \ldots, \beta_{k+1}) \notin M_0$, we get (from the definition of M_0) that there exists $j \in \mathbb{N}$ such that $j < \beta_1$ and $(j, \beta_2, \ldots, \beta_{k+1}) \in M_0$ contradicting thus the minimality of $(\beta_1, \ldots, \beta_{k+1})$ in S.

Case 2. $(\beta_2, \ldots, \beta_{k+1}) \notin M_1$, i.e. $(\beta_2, \ldots, \beta_{k+1})$ is not a minimal element of S_1.

In this case, there exists $(\gamma_1, \overline{\gamma_1}) \in M_0$ such that $\overline{\gamma_1} \prec_k (\beta_2, \ldots, \beta_{k+1})$. Now, since we assumed that $(\beta_1, \ldots, \beta_{k+1})$ is a minimal element of S, we obtain that $\beta_1 < \gamma_1 \leq \ell$. Since we assumed that $(\beta_1, \ldots, \beta_{k+1}) \notin M_{0,\beta_1}$, then there exists $(\beta_1, \ldots, \beta_{k+1}) \neq (\beta_1, \overline{\beta_1}) \in M_{0,\beta_1}$ such that $\overline{\beta_1} \prec_k (\beta_2, \ldots, \beta_{k+1})$, and thus $(\beta_1, \overline{\beta_1}) \prec_{k+1} (\beta_1, \beta_2 \ldots, \beta_{k+1})$ contradicting our assumption on the minimality of $(\beta_1, \ldots, \beta_{k+1})$.

Therefore M is a finite set containing all minimal elements of S. $\quad\square$

In particular, Proposition 2.3 yields the following result.

Proposition 2.4. *Let $H \subset \mathbb{Z}^r$ be a subgroup. Then $H \cap \mathbb{N}^r$ is a finitely generated semigroup of $\mathbb{N}^r$.*

Proof. Assume $S := H \cap \mathbb{N}^r$ is not the trivial semigroup (in which case our claim is vacuously true). Hence, let M be the finite set of all minimal elements with respect to $\prec$ of $S \setminus \{(0, \ldots, 0)\}$. We claim that S is the semigroup generated by M.

Indeed, assume the semigroup S_0 generated by M is not equal to S. Clearly $S_0 \subset S$ since S is the intersection of $\mathbb{N}^r$ with a subgroup of $\mathbb{Z}^r$. Let γ be a minimal element with respect to $\prec$ of $S \setminus S_0$. Since $(0, \ldots, 0) \neq \gamma \notin M$, we conclude that there exists $\gamma \neq \beta \in M \subset S_0$ such that $\beta \prec \gamma$. But then $\gamma - \beta \in \mathbb{N}^r$ and since both β and γ are also in H, we get that $\gamma - \beta \in S$. Since $\gamma \notin S_0$, then also $\gamma - \beta \notin S_0$, but on the other hand $\gamma \neq (\gamma - \beta) \prec \gamma$ contradicting thus the minimality of γ.

This concludes our proof that S is generated as a subsemigroup of $\mathbb{N}^r$ by the finite set M. $\quad\square$

The following propositions yield additional properties of subsemigroups of $\mathbb{N}^r$.

Proposition 2.5. *For any subgroup $H \subset \mathbb{Z}^r$, and for any $\gamma \in \mathbb{Z}^r$, the intersection $(\gamma + H) \cap \mathbb{N}^r$ is a union of at most finitely many cosets of subsemigroups of the form $\beta + (H \cap \mathbb{N}^r)$.*

Proof. We let M be the finite set (see Proposition 2.3) of minimal elements with respect to $\prec$ for the set $(\gamma + H) \cap \mathbb{N}^r$. We claim that

$$(\gamma + H) \cap \mathbb{N}^r = \bigcup_{\beta \in M} \beta + (H \cap \mathbb{N}^r).$$

Indeed, the reverse inclusion is immediate. Now, for the direct inclusion, if $\tau \in (\gamma + H) \cap \mathbb{N}^r$, then there exists $\beta \in M$ such that $\beta \prec \tau$. So, $\tau - \beta \in \mathbb{N}^r$. On the other hand, since both β and τ are in $\gamma + H$, we also get that $\tau - \beta \in H$, as desired. $\qquad\square$

Proposition 2.6. *For any $\gamma_1, \gamma_2 \in \mathbb{N}^r$ and for any subgroups $H_1, H_2 \subset \mathbb{Z}^r$, the intersection $(\gamma_1 + (H_1 \cap \mathbb{N}^r)) \cap (\gamma_2 + (H_2 \cap \mathbb{N}^r))$ is a union of at most finitely many cosets of subsemigroups of the form $\beta + (H \cap \mathbb{N}^r)$, where $H := H_1 \cap H_2$.*

Proof. We let M be the finite set (see Proposition 2.3) of minimal elements with respect to $\prec$ for the set $(\gamma_1 + (H_1 \cap \mathbb{N}^r)) \cap (\gamma_2 + (H_2 \cap \mathbb{N}^r))$. We claim that

$$(\gamma_1 + (H_1 \cap \mathbb{N}^r)) \cap (\gamma_2 + (H_2 \cap \mathbb{N}^r)) = \bigcup_{\beta \in M} \beta + (H \cap \mathbb{N}^r).$$

Indeed, the reverse inclusion is immediate. Now, for the direct inclusion, if $\tau \in (\gamma_1 + (H_1 \cap \mathbb{N}^r)) \cap (\gamma_2 + (H_2 \cap \mathbb{N}^r))$, then there exists $\beta \in M$ such that $\beta \prec \tau$. So, $\tau - \beta \in \mathbb{N}^r$. On the other hand, since both β and τ are in $\gamma_1 + H_1$ and in $\gamma_2 + H_2$, we also get that $\tau - \beta \in H_1 \cap H_2 = H$, as desired. $\qquad\square$

Proposition 2.7. *Let $\gamma \in \mathbb{N}^r$, let $H \subset \mathbb{Z}^r$ be a subgroup, and let $N \in \mathbb{N}$ be a positive integer. Assume that for a subset $L \subset (\gamma + H \cap \mathbb{N}^r)$, we have that for each $\tau \in H \cap \mathbb{N}^r$, and for each $\beta \in L$, then also $\beta + N \cdot \tau \in L$. Then L is a union of at most finitely many cosets of subsemigroups of the form $\delta + ((N \cdot H) \cap \mathbb{N}^r)$.*

Proof. Since $H / N \cdot H$ is finite, we may write H as a finite union $\bigcup_{i=1}^{s} \tau_i + N \cdot H$ for some $\tau_i \in \mathbb{Z}^r$. Using Proposition 2.5, we conclude that each

$$\gamma + (\tau_i + N \cdot H) \cap \mathbb{N}^r$$

is itself in the class $\mathcal{C}$ (see Definition 2.1); more precisely we may write

$$\gamma + H \cap \mathbb{N}^r = \bigcup_{i=1}^{s} (\gamma + (\tau_i + N \cdot H) \cap \mathbb{N}^r) = \bigcup_{\beta \in M} (\beta + ((N \cdot H) \cap \mathbb{N}^r)),$$

for a suitable finite subset M of $\mathbb{N}^r$. Therefore, it suffices to show that for each $\beta \in M$, the set

$$L_\beta := L \cap (\beta + ((N \cdot H) \cap \mathbb{N}^r))$$

satisfies the conclusion of our Proposition 2.7. Now, for each such $\beta \in M$, we let M_β be the finite set of minimal elements of L_β with respect to the ordering $\prec$ of $\mathbb{N}^r$. Then, according to our hypothesis, we do have that

$$\bigcup_{\delta \in M_\beta} (\delta + ((N \cdot H) \cap \mathbb{N}^r)) \subset L_\beta.$$

We claim that the above inclusion is in fact an equality. Indeed, for any $\zeta \in L_\beta$, there exists $\delta \in M_\beta$ such that $\delta \prec \zeta$. Therefore $\zeta - \delta \in \mathbb{N}^r$. On the other hand, both ζ and δ are in $\beta + N \cdot H$, which means that $\zeta - \delta \in N \cdot H$, and thus $\zeta - \delta \in (N \cdot H) \cap \mathbb{N}^r$, as desired. □

Proposition 2.8. *Let* $\pi_1 : \mathbb{N}^r \longrightarrow \mathbb{N}$ *be the projection on the first coordinate, and let* $\pi_{2,\dots,r} : \mathbb{N}^r \longrightarrow \mathbb{N}^{r-1}$ *be the projection on the last* $(r-1)$ *coordinates. Then for each* $a \in \mathbb{N}$, *for each* $\gamma \in \mathbb{N}^r$ *and for each subgroup* $H \subset \mathbb{Z}^r$, *we have that* $\pi_{2,\dots,r}\left(\pi_1^{-1}(a) \cap (\gamma + H \cap \mathbb{N}^r)\right)$ *is in the class* $\mathcal{C}$.

Proof. Using Propositions 2.5 and 2.6 we may assume that $\gamma + (H \cap \mathbb{N}^r) \subset \pi_1^{-1}(a)$ since $\pi_1^{-1}(a)$ is itself in the class $\mathcal{C}$, and thus its intersection with $\gamma + H \cap \mathbb{N}^r$ is again in the class $\mathcal{C}$. The conclusion of Proposition 2.8 follows since the projection of any subgroup is also a subgroup. □

Proposition 2.9. *Let* $L \subset \mathbb{N}^r$, *and let* $\beta := (\beta_1, \dots, \beta_r) \in L$. *For each* $i = 1, \dots, r$ *and for each* $j = 0, \dots, \beta_i - 1$, *we let*

$$L_{i,j} := \{(\gamma_1, \dots, \gamma_r) \in L : \gamma_i = j\} \quad and \quad L_\beta := \{\gamma \in L : \beta \prec \gamma\}.$$

Then

$$(2.10) \qquad\qquad L = L_\beta \bigcup \left(\bigcup_{i,j} L_{i,j}\right).$$

Moreover, if L *is in the class* $\mathcal{C}$, *then each* $L_{i,j}$ *and* L_β *are in the class* $\mathcal{C}$.

Proof. The decomposition of L as in (2.10) follows from the definition of the ordering $\prec$ on $\mathbb{N}^r$. The "moreover" claim follows from Proposition 2.8 – note that $L_\beta \in \mathcal{C}$ because

$$L_\beta = L \cap (\beta + \mathbb{N}^r),$$

and according to Proposition 2.6, the class $\mathcal{C}$ is closed under taking the intersection of any two elements of it. □

Using the results of this Section we can prove that Question 1.4 *always* has a positive answer when V is zero-dimensional. This result will be used in the inductive hypothesis from the proof of Lemma 3.2.

Proposition 2.11. *Let* X *be any quasiprojective variety defined over an arbitrary field* K, *let* $\Phi_1, \dots, \Phi_r$ *be any set of commuting endomorphisms of* X, *let* $\alpha \in X(K)$, *and let* V *be a zero-dimensional subvariety of* X. *Then the set of tuples* $(n_1, \dots, n_r) \in \mathbb{N}^r$ *for which* $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V$ *belongs to the class* $\mathcal{C}$.

Proof. Obviously, it suffices to prove our result assuming V consists of a single point, call it β. We let E be the set of all tuples $(n_1, \dots, n_r) \in \mathbb{N}^r$ such that $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) = \beta$. According to Proposition 2.3, the set E has

a finite set M of minimal elements with respect to the ordering $\prec$ on $\mathbb{N}^r$. Now, let

$$L := \{(n_1, \ldots, n_r) \in \mathbb{N}^r : \Phi_1^{n_1} \cdots \Phi_r^{n_r}(\beta) = \beta\}.$$

Let H be the subgroup of $\mathbb{Z}^r$ generated by L. We claim that $L = H \cap \mathbb{N}^r$. Indeed, we see from the definition of L that it is closed under addition, and moreover, for any $\beta, \gamma \in L$ such that $\beta \prec \gamma$, then also $\gamma - \beta \in L$. Now it is immediate to see that $E = \bigcup_{\tau \in M}(\tau + L)$, as desired. □

The following result is an immediate corollary of Proposition 2.11 and Theorem 1.1, which shows that Question 1.2 has positive answer assuming G is a *simple* semiabelian variety (i.e. G has no connected algebraic subgroups other than itself, and the trivial algebraic group).

Corollary 2.12. *Let G be a simple semiabelian variety defined over $\mathbb{C}$, let $\Phi_1, \ldots, \Phi_r$ be any set of commuting endomorphisms of G, let $\alpha \in G(\mathbb{C})$, and let V be any subvariety of G. Then the set of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V$ belongs to the class $\mathcal{C}$.*

We will use the following easy lemma both in the proof of Corollary 2.12, and also in the proof of our main result Theorem 1.3.

Lemma 2.13. *Let G be a semiabelian variety defined over $\mathbb{C}$, let S be a commutative semigroup of $\operatorname{End}(G)$ generated by the endomorphisms $\Phi_1, \ldots, \Phi_r$ of G, and let $\alpha \in G(\mathbb{C})$. Then the orbit $\mathcal{O}_S(\alpha)$ spans a finitely generated subgroup Γ of $G(\mathbb{C})$.*

Proof. Each endomorphism Ψ of G satisfies a monic equation of degree $2\ell + k$ over $\mathbb{Z}$ (seen as a subring of $\operatorname{End}(G)$), where $1 \to \mathbb{G}_m^k \to G \to A \to 1$ is exact and $l = \dim A$. This follows by taking the characteristic polynomial of the action Ψ induces on $H_1(G, \mathbb{Z})$, which has dimension equal to $2\ell + k$ (see [16, I.10], for example). Hence $\mathcal{O}_S(\alpha)$ is contained in the subgroup $\Gamma \subset G(\mathbb{C})$ spanned by all $\Phi_1^{n_1} \ldots \Phi_r^{n_r}(\alpha)$ where $0 \le n_i < 2\ell + k$ for each $i = 1, \ldots, r$. □

Proof of Corollary 2.12. It is clear that it suffices to prove Corollary 2.12 assuming V is irreducible. Furthermore, we may replace V by the Zariski closure of $V(\mathbb{C}) \cap \mathcal{O}_S(\alpha)$.

If there are only finitely many distinct points in the intersection of V with the orbit $\mathcal{O}_S(\alpha)$ under the semigroup S generated by $\Phi_1, \ldots, \Phi_r$, then we are done by applying Proposition 2.11 to each of the finitely many points in $V(\mathbb{C}) \cap \mathcal{O}_S(\alpha)$.

Now, assume $V(\mathbb{C}) \cap \mathcal{O}_S(\alpha)$ is infinite. Then also $V(\mathbb{C}) \cap \Gamma$ is infinite, where Γ is the subgroup of $G(\mathbb{C})$ generated by $\mathcal{O}_S(\alpha)$ (by Lemma 2.13, we know that Γ is a finitely generated subgroup). Applying Theorem 1.1, we conclude that the irreducible subvariety V is the Zariski closure of a coset of an infinite subgroup of Γ; therefore, we conclude that V is a translate of a

connected algebraic subgroup of G. However, since G is a simple semiabelian variety, and since V contains infinitely many points (because $V(\mathbb{C}) \cap \mathcal{O}_S(\alpha)$ is infinite), we conclude that $V = G$. Then the conclusion of Corollary 2.12 is immediate. $\qquad\square$

Corollary 2.12 immediately yields Theorem 1.3(c) for $j = 0, 1$ (note that each one-dimensional semiabelian variety is simple).

Corollary 2.14. *Let A be a simple semiabelian variety, let $j \in \{0, 1\}$, and let $G = A^j$. Let $\Phi_1, \ldots, \Phi_r$ be any set of commuting endomorphisms of G, let $\alpha \in G(\mathbb{C})$, and let V be any subvariety of G. Then the set of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V$ belongs to the class $\mathcal{C}$.*

3. Some reductions

In this section, we will show that it suffices to prove Theorem 1.3 in the case where the Φ_i are all finite maps and where α has been replaced by a suitable multiple $m\alpha$. This will allow us in Section 4 to use p-adic logarithms and exponentials to translate our problem into the language of linear algebra.

Lemma 3.1. *It suffices to prove Theorem 1.3 if each Φ_i is finite.*

Proof of Lemma 3.1. We proceed by induction on the number r of generators of the semigroup S; the case $r = 0$ is trivial since then the semigroup S is trivial.

Assume $r = 1$, i.e. $S = \langle \Phi_1 \rangle$. Because $\Phi_1^n(G) \subset \Phi_1^{n-1}(G)$ for each $n \in \mathbb{N}$, and because there is no infinite descending chain of semiabelian varieties, we conclude that there exists $N_1 \in \mathbb{N}$ such that Φ_1 is a finite endomorphism of the semiabelian variety $G_1 := \Phi_1^{N_1}(G)$. Hence, replacing G by G_1, replacing V by $V \cap G_1$, and replacing α by $\Phi_1^{N_1}(\alpha)$ we are done.

In the above argument, note that if we are in the case of Theorem 1.3(c) and $G = A^2$, where A is a one-dimensional semiabelian variety, in the above descending chain of semiabelian varieties one may only find the trivial group, or the group G itself, or some one-dimensional semiabelian variety. Indeed, $\dim(G) = 2$, and thus, each proper semiabelian subvariety of G is one-dimensional. Therefore, in the argument from the above paragraph, if G satisfies the hypothesis of Theorem 1.3(c), then also each semiabelian subvariety $\Phi_1^i(G)$ would also satisfy the hypothesis of Theorem 1.3(c).

Assume that we proved Lemma 3.1 for all semigroups S generated by fewer than r endomorphisms. Reasoning as before, for each $i = 1, \ldots, r$ we find $N_i \in \mathbb{N}$ such that Φ_i is a finite endomorphism of the semiabelian variety $G_i := \Phi_i^{N_i}(G)$; let $H := \Phi_1^{N_1} \cdots \Phi_r^{N_r}(G)$. Then Proposition 2.9 applied to the element $(N_1, \ldots, N_r)$ of $\mathbb{N}^r$ allows us to apply the inductive hypothesis. More precisely, for each $i = 1, \ldots, r$, we let S_i be the commutative

semigroup generated by all Φ_j for $j \neq i$; then

$$\mathcal{O}_S(\alpha) = \mathcal{O}_S(\Phi_1^{N_1} \cdots \Phi_r^{N_r}(\alpha))$$

$$\bigcup \left(\mathcal{O}_{S_1}(\alpha) \cup \mathcal{O}_{S_1}(\Phi_1(\alpha)) \cup \cdots \cup \mathcal{O}_{S_1}(\Phi_1^{N_1-1}(\alpha)) \right)$$

$$\bigcup \left(\mathcal{O}_{S_2}(\alpha) \cup \mathcal{O}_{S_2}(\Phi_2(\alpha)) \cup \cdots \cup \mathcal{O}_{S_2}(\Phi_2^{N_2-1}(\alpha)) \right)$$

$$\bigcup \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\bigcup \left(\mathcal{O}_{S_r}(\alpha) \cup \mathcal{O}_{S_r}(\Phi_r(\alpha)) \cup \cdots \cup \mathcal{O}_{S_r}(\Phi_r^{N_r-1}(\alpha)) \right).$$

Each S_i is generated by $(r-1)$ endomorphisms of G, and thus, by the induction hypothesis, Lemma 3.1 holds for the intersection of the subvariety V with each S_i-orbit. On the other hand, each Φ_i is finite on H, and $\Phi_1^{N_1} \cdots \Phi_r^{N_r}(\alpha) \in H(\mathbb{C})$; so, replacing G by H, and replacing V by $V \cap H$, we are done. $\qquad\square$

From now on in the proof of Theorem 1.3 (and thus in this Section), we assume each Φ_i is finite on G. Clearly, it suffices to prove Theorem 1.3 for irreducible subvarieties V.

Next we prove another important reduction.

Lemma 3.2. *It suffices to prove Theorem 1.3 for the S-orbit of $m\alpha$, and for the variety mV, where m is any positive integer.*

Proof. We will prove an (apparently) even stronger statement; we will show that for any coset of a subsemigroup of the form $\gamma + F \cap \mathbb{N}^r$ (where $\gamma \in \mathbb{N}^r$ and $F \subset \mathbb{Z}^r$ is a subgroup), the set of tuples $(n_1, \ldots, n_r) \in (\gamma + F \cap \mathbb{N}^r)$ for which $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V(\mathbb{C})$ belongs to the class $\mathcal{C}$. On the other hand, this apparent stronger statement is equivalent with the original one. Indeed, if we know that the set of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V(\mathbb{C})$ belongs to the class $\mathcal{C}$, then Proposition 2.6 yields that also when we restrict to those tuples which are in $\gamma + F \cap \mathbb{N}^r$, we also get a set from the class $\mathcal{C}$. So, from now on, we let S be the set of all endomorphisms

$$\{\Phi_1^{n_1} \cdots \Phi_r^{n_r} : (n_1, \ldots, n_r) \in (\gamma + F \cap \mathbb{N}^r)\}.$$

We proceed the proof of Lemma 3.2 by induction on $\dim(V) + r$; the case $\dim(V) = r = 0$ is obvious. Note also that if $\dim(V) = 0$, then Theorem 1.3 was already proved in higher generality in Proposition 2.11. On the other hand, if $r = 0$, then the semigroup S is trivial, and so the statement of Theorem 1.3 is obvious without any conditions. Furthermore, if $r = 1$, then Theorem 1.3 is true in more generality, as shown in [7].

Now, fix a positive integer m and suppose that Theorem 1.3 is true for the intersection of the S-orbit of $m\alpha$ with the variety mV. So, we know that there exists a set $E_m \in \mathcal{C}$ which contains all tuples $(n_1, \ldots, n_r) \in$

$(\gamma + F \cap \mathbb{N}^r)$ such that

$$\Phi_1^{n_1} \cdots \Phi_r^{n_r}(m\alpha) \in mV.$$

For every $\Psi \in S$ such that $\Psi(\alpha) \in V$, we have $\Psi(m\alpha) \in mV$ (because Ψ is an algebraic group endomorphism). Therefore, if E is the set of tuples $(n_1, \ldots, n_r) \in (\gamma + F \cap \mathbb{N}^r)$ for which

$$\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in V,$$

then $E \subset E_m$. Let $\beta + (H \cap \mathbb{N}^r)$, where $\beta \in \mathbb{N}^r$ and H is a subgroup of $\mathbb{Z}^r$, be one of the cosets of subsemigroups contained in E_m; by definition of the class $\mathcal{C}$, we know that E_m is a finite union of such cosets of subsemigroups. It suffices to show that $E \cap (\beta + (H \cap \mathbb{N}^r)) \in \mathcal{C}$.

For β and H as above, we let

$$S_1 := \{\Phi^{n_1} \cdots \Phi_r^{n_r} : (n_1, \ldots, n_r) \in H \cap \mathbb{N}^r\},$$

and we let $\alpha_1 := \Phi_1^{b_1} \cdots \Phi_r^{b_r}(\alpha)$, where $\beta := (b_1, \ldots, b_r)$. Clearly, it suffices to show that the set E_β of tuples $(n_1, \ldots, n_r) \in H \cap \mathbb{N}^r$ for which

$$\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha_1) \in V(\mathbb{C})$$

belongs to the class $\mathcal{C}$.

We let V_1 be the Zariski closure of $\mathcal{O}_{S_1}(\alpha_1)$. If V is not contained in V_1, then $V \cap V_1$ has smaller dimension than V (since V is irreducible), and because

$$V(\mathbb{C}) \cap \mathcal{O}_{S_1}(\alpha_1) = (V \cap V_1)(\mathbb{C}) \cap \mathcal{O}_{S_1}(\alpha_1),$$

we are done by the induction hypothesis (also note that if we are in part (b) of Theorem 1.3, then $V \cap V_1$ is zero-dimensional, and thus the conclusion follows as shown in Proposition 2.11).

Assume now that $V \subset V_1$. Since, by construction, $m \cdot \mathcal{O}_{S_1}(\alpha_1) \subset mV$ (because each Φ_i is an algebraic group endomorphism), we have that $mV_1 \subset mV$. Therefore, $\dim(V) = \dim(V_1)$, and moreover V is an irreducible component of V_1. For each $\sigma \in S_1$, we have $\sigma(V_1) \subset V_1$ since $\sigma(\mathcal{O}_{S_1}(\alpha_1)) \subset \mathcal{O}_{S_1}(\alpha_1)$. Furthermore, since each σ is a finite map, we conclude that σ maps each irreducible component of V_1 of maximal dimension into another such component; hence V is preperiodic under σ. There are two cases, which are covered in the following two propositions.

Proposition 3.3. *If there exists $\sigma \in S_1$ such that V is not periodic under σ, then $E_\beta \in \mathcal{C}$.*

Proof. First of all, at the expense of replacing σ by an iterate, we may assume that $V \not\subset \sigma(V_1)$ (since σ maps the finite set of irreducible components of V_1 of maximal dimension into itself, but no power of σ preserves V).

We let $(k_1, \ldots, k_r) \in \mathbb{N}^r$ such that $\sigma = \Phi_1^{k_1} \cdots \Phi_r^{k_r}$. We apply Proposition 2.9 to the element $(k_1, \ldots, k_r)$ of the set $H \cap \mathbb{N}^r$ and construct the subsets:

$$H_{(k_1,\ldots,k_r)} := \{\gamma \in H \cap \mathbb{N}^r : (k_1, \ldots, k_r) \prec \gamma\}$$

and

$$H_{i,j} := \{(\ell_1, \ldots, \ell_r) \in H \cap \mathbb{N}^r : \ell_i = j\},$$

for $i = 1, \ldots, r$ and for $0 \le j < k_i$. Then, as in Proposition 2.9, we have

$$H \cap \mathbb{N}^r = H_{(k_1,\ldots,k_r)} \bigcup \left(\bigcup_{\substack{1 \le i \le r \\ 0 \le j \le k_i - 1}} H_{i,j} \right).$$

It suffices to show that $E_\beta \cap H_{(k_1,\ldots,k_r)} \in \mathcal{C}$ and also that each $E_\beta \cap H_{i,j} \in \mathcal{C}$.

Propositions 2.9 and 2.8 show that the projection of each $H_{i,j}$ on the $(r-1)$-st coordinates of $\mathbb{N}^r$ other than the i-th coordinate is also in the class $\mathcal{C}$. Therefore the intersection $E_\beta \cap H_{i,j}$ belongs to the class $\mathcal{C}$ by the inductive hypothesis, since we reduced the original problem to the intersection between the subvariety V with the orbit of a point under a finitely generated commuting semigroup based on $(r-1)$ endomorphisms of G.

Now, for each $(\ell_1, \ldots, \ell_r) \in H_{(k_1,\ldots,k_r)} \cap E_\beta$, we actually have that

$$\Phi_1^{\ell_1} \cdots \Phi_r^{\ell_r}(\alpha_1) \in (V \cap \sigma(V_1))(\mathbb{C}),$$

because $(k_1, \ldots, k_r) \prec (\ell_1, \ldots, \ell_r)$ and $\sigma = \Phi_1^{k_1} \cdots \Phi_r^{k_r}$. Since V is an irreducible variety and $V \not\subset \sigma(V_1)$, we conclude that $V \cap \sigma(V_1)$ has smaller dimension than $\dim(V)$. Thus $E_\beta \cap H_{(k_1,\ldots,k_r)} \in \mathcal{C}$ by our induction hypothesis, since we reduced the original problem to the intersection between the orbit of a point under a finitely generated commuting semigroup based on r endomorphisms of G with a subvariety of dimension less than $\dim(V)$. $\square$

Proposition 3.4. *If for each $\sigma \in S_1$, the variety V is periodic under σ, then $E_\beta \in \mathcal{C}$.*

Proof. According to Proposition 2.4, there are finitely many generators $\{\tau_i\}_{1 \le i \le s}$ for $H \cap \mathbb{N}^r$. For each $i = 1, \ldots, s$, we let $\sigma_i \in S_1$ be the element of S_1 corresponding to τ_i; more precisely, if $\tau_i := (k_1, \ldots, k_r)$, then we let $\sigma_i := \Phi_1^{k_1} \cdots \Phi_r^{k_r}$.

Using the hypothesis of Proposition 3.4, for each $i = 1, \ldots, s$, we let $N_i \in \mathbb{N}$ such that $\sigma_i^{N_i}(V) = V$. We let N be the least common multiple of all these N_i. Then $\sigma^N(V) = V$ for all $\sigma \in S_1$ (since $H \cap \mathbb{N}^r$ is generated by the τ_i's). In particular, we get that if $\gamma \in E_\beta$, and if $\tau \in H \cap \mathbb{N}^r$, then $\gamma + N \cdot \tau \in E_\beta$. The conclusion of Proposition 3.4 follows from Proposition 2.7. $\square$

Propositions 3.3 and 3.4 finish the proof of Lemma 3.2. $\square$

4. The p-adic uniformization

We continue with the notation (and the reductions) from Section 3.

Let Γ be the subgroup of $G(\mathbb{C})$ spanned by $\mathcal{O}_S(\alpha)$ (see Lemma 2.13). Theorem 1.1 yields that $V(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ. The Zariski closure of each coset of a subgroup of Γ is a a translate of an algebraic subgroup of G. Hence, it suffices to describe the intersection $\mathcal{O}_S(\alpha) \cap G_1(\mathbb{C})$, where $G_1 = \beta + G_0$ is a translate of a connected algebraic subgroup G_0 of G.

Let R be a finitely generated extension of $\mathbb{Z}$ over which G, G_0, and each Φ_i can be defined. By [2, Proposition 4.4] (see also [7, Proposition 3.3]), there exists a p and an embedding of R into $\mathbb{Z}_p$ such that

(1) G and G_0 have smooth models $\mathcal{G}$ and $\mathcal{G}_0$ over $\mathbb{Z}_p$;
(2) each Φ_i extends to an unramified endomorphism of $\mathcal{G}$;
(3) α and β extend to points in $\mathcal{G}(\mathbb{Z}_p)$.

Let J_i denote the map Φ_i induces on the tangent space of 0. By (2) and [2, Proposition 2.2], if one chooses coordinates for this tangent space via generators for the completed local ring at 0, then the entries of the matrix for J_i will be in $\mathbb{Z}_p$. Fix one such set of coordinates and let $|\cdot|_p$ denote the corresponding p-adic metric on the tangent space at 0.

According to [4, Proposition 3, p. 216] there exists a p-adic analytic map exp which induces an analytic isomorphism between a sufficiently small neighborhood $\mathcal{U}$ of $\mathbb{G}_a^g(\mathbb{C}_p)$ and a corresponding p-adic neighborhood of the origin $0 \in \mathcal{G}(\mathbb{C}_p)$. Furthermore (at the expense of possibly replacing $\mathcal{U}$ by a smaller set), we may assume that the neighborhood $\mathcal{U}$ is a sufficiently small open ball, i.e., there exists a (sufficiently small) positive real number ϵ such that $\mathcal{U}$ consists of all $(z_1, \ldots, z_g) \in \mathbb{C}_p^g$ satisfying $|z_i|_p < \epsilon$. Because $\exp(\mathcal{U}) \cap \mathcal{G}(\mathbb{Z}_p)$ is an open subgroup of the compact group $\mathcal{G}(\mathbb{Z}_p)$ (see [7]), we conclude that $\exp(\mathcal{U}) \cap \mathcal{G}(\mathbb{Z}_p)$ has finite index m in $\mathcal{G}(\mathbb{Z}_p)$. So, at the expense of replacing α by $m\alpha$, and G_1 by $mG_1 = m\beta + mG_0$ (which is allowed by Lemma 3.2) we may assume that $\alpha, \beta \in \exp(\mathcal{U})$. Therefore, there exists $u_0, v_0 \in \mathcal{U}$ such that $\exp(u_0) = \alpha$ and $\exp(v_0) = \beta$. Furthermore, for each $i = 1, \ldots, r$, and for each $z \in \mathcal{U}$ we have $\exp(J_i z) = \Phi_i(\exp(z))$, since exp induces a local p-adic analytic isomorphism between $\mathbb{C}_p^g$ and $\mathcal{G}(\mathbb{C}_p)$. Finally, there exists a linear subvariety $\mathcal{V} \subset \mathbb{G}_a^g$ such that $\exp(\mathcal{V}(\mathcal{U}))$ is a p-adic neighborhood of the origin $0 \in \mathcal{G}_0(\mathbb{C}_p)$.

Thus we reduced Theorem 1.3 to proving the following result.

Proposition 4.1. *In order to prove Theorem 1.3, it suffices to show that the set E of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $J_1^{n_1} \cdots J_r^{n_r}(u_0) \in (v_0 + \mathcal{V})$ belongs to the class $\mathcal{C}$.*

Proof. Since the entries of each J_i are in $\mathbb{Z}_p$, we have $J_i(\mathcal{U}) \subset \mathcal{U}$ for each $i = 1, \ldots, r$ (also note the fact that $\mathcal{U}$ is an open ball given by the norm

inequalities $|z_i|_p < \epsilon$ for each coordinate z_i). So, for each $(n_1, \ldots, n_r) \in \mathbb{N}^r$ we have $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) \in (\beta + \mathcal{G}_0(\mathbb{C}_p))$ if and only if

$$J_1^{n_1} \ldots J_r^{n_r}(u_0) \in v_0 + \mathcal{V},$$

since $\Phi_1^{n_1} \cdots \Phi_r^{n_r}(\alpha) = \exp{(J_1^{n_1} \cdots J_r^{n_r}(u_0))}$. $\qquad\qquad\square$

5. Proof of our main result

We continue with the notation and reductions from the previous two Sections.

5.1. Proof of Theorem 1.3(a). Because the matrices J_i are all diagonalizable and all commute, they must be simultaneously diagonalizable. To see this, note that if E_λ is a λ-eigenspace for a transformation T, and U is a transformation that commutes with T, then $UE_\lambda \subseteq E_\lambda$ since for any w in E_λ we have $T(Uw) = UTw = U(\lambda w) = \lambda Uw$. Hence the J_i admit a common decomposition into eigenspaces and, therefore, a common eigenbasis.

Let C be an invertible matrix such that $C^{-1}J_iC = B_i$ is diagonal for each $i = 1, \ldots, r$. Letting $u_1 := C^{-1}u_0$, and $v_1 := C^{-1}v_0$, and $\mathcal{V}_1 := C^{-1}\mathcal{V}$, Proposition 4.1 reduces to describing the set of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ satisfying

$$(5.1) \qquad\qquad B_1^{n_1} \ldots B_r^{n_r}(u_1) \in v_1 + \mathcal{V}_1.$$

Using Theorem 1.1 for the algebraic torus $\mathbb{G}_m^g$ and its linear subvariety $v_1 + \mathcal{V}_1$, we conclude that the set of tuples $(n_1, \ldots, n_r)$ satisfying (5.1) lie in the intersection of $\mathbb{N}^r$ with a finite union of cosets of subgroups of $\mathbb{Z}^r$. According to Proposition 4.1, this concludes the proof of Theorem 1.3(a) (see also Proposition 2.5).

5.2. Proof of Theorem 1.3(b). In this case, in Proposition 4.1 we know in addition that $v_0 = 0$ (since the subvariety V is a connected algebraic group, not a translate of it), and furthermore, the linear subvariety $\mathcal{V}$ is actually just a line L passing through the origin (since the algebraic subgroup has dimension equal to one).

The following simple result will give rise to a proof of Theorem 1.3(b).

Proposition 5.2. *Let V be a vector space over a field of characteristic 0, let T be a group of invertible linear transformations of V, let $v \in V$, let Z be a one-dimensional subspace of V, and let*

$$\mathcal{S} = \{g \in T : g(v) \in Z\}.$$

If $\mathcal{S}$ is nonempty, then $\mathcal{S}$ is a right coset of a subgroup of T.

Proof. If v is the zero vector, then the result is immediate. So, from now on, assume that v is nonzero.

Let $T_Z = \{g \in T : g(Z) = Z\}$ be the subgroup of G which stabilizes the linear subspace Z. If $\mathcal{S}$ is not empty, we may choose some $a \in \mathcal{S}$. Then for any $b \in \mathcal{S}$, we have $ba^{-1}(a(v)) \in Z$. Since $a(v) \neq 0$ and ba^{-1} is linear this means that $ba^{-1} \in T_Z$. Thus, b is in the coset $T_Z a$. Similarly, $ga(v) \in Z$ for any $ga \in T_Z a$. Thus, $\mathcal{S} = T_Z a$. $\qquad\square$

Now we are ready to finish the proof of Theorem 1.3(b).

Let T be the group of matrices generated by the J_i (note that each J_i is invertible since each Φ_i is a finite map by the reduction proved in Lemma 3.1). Then, by Proposition 5.2, the set of $g \in T$ such that $g(u_0) \in L$ is a coset $T_L a$ of a subgroup T_L of T which stabilizes the one dimensional variety L. Now, for $i = 1, \ldots, r$, let e_i be the element of $\mathbb{Z}^r$ whose j-th coordinate is the Kronecker delta δ_{ij}. Let ρ be the map from $\mathbb{Z}^r$ to T that takes e_i to J_i. Then $\rho^{-1}(T_L a)$ is a coset $\gamma + H$ of a subgroup $H \subset \mathbb{Z}^r$. This shows that the set E of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ for which $J_1^{n_1} \cdots J_r^{n_r}(u_0) \in L$ is in fact $(\gamma + H) \cap \mathbb{N}^r$. Using Proposition 2.5 we obtain that $E \in \mathcal{C}$, as desired in the conclusion of Proposition 4.1. This concludes the proof of Theorem 1.3(b).

Remark. Although Proposition 5.2 holds for *any* group T (not just finitely generated commutative groups T), Lemma 3.1 only holds for finitely generated commutative semigroups S, so we are only able to reduce to Proposition 5.2 under the assumption that our semigroup is commutative and finitely generated. On the other hand, if the semigroup is finitely generated and all of its elements are finite, then the proof of Theorem 1.3(b) should go through, even when the semigroup is not commutative. The case of semigroups that are not finitely generated is more troublesome; for example, it may not be possible to find a p such that all of the generators are defined over $\mathbb{Z}_p$.

5.3. Proof of Theorem 1.3(c).
We already proved Theorem 1.3(c) when $G = A^j$ for $j < 2$ in Corollary 2.14 (note that a one-dimensional semiabelian variety is clearly simple). Therefore, from now on, we may assume $G = A^2$.

Since it is a one-dimensional semiabelian variety, A is either isomorphic to $\mathbb{G}_m$ or to an elliptic curve E. In either case, $\mathrm{End}(E)$ is isomorphic with a subring $\mathcal{R}$ of the ring $\mathfrak{O}_K$ of algebraic integers in a given quadratic imaginary field K. We already proved the result if (for each i) the Jacobian J_i of Φ_i at the identity of A^2 is diagonalizable. Therefore, we may assume there exists at least one such Jacobian which is not diagonalizable. Since the endomorphism ring of A^2 is isomorphic with the ring $M_{2,2}(\mathcal{R})$ of 2-by-2 matrices with integer coefficients, we have that each $J_i \in M_{2,2}(\mathcal{R})$.

The following result is an elementary application of linear algebra.

Proposition 5.3. *Let $J_1, \ldots, J_r \in M_{2,2}(\mathcal{R})$ be commuting 2-by-2 matrices. Assume there exists $i = 1, \ldots, r$ such that J_i is not diagonalizable. Then there exists an invertible 2-by-2 matrix B defined over K such that for each $i = 1, \ldots, r$ there exist $a_i \in \mathfrak{O}_K$ and $c_i \in K$ such that*

$$B J_i B^{-1} = a_i \cdot \begin{pmatrix} 1 & c_i \\ 0 & 1 \end{pmatrix}.$$

Proof. Note in general that if $\lambda_1 \neq \lambda_2$, then $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ commutes with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ if and only if $c = b = 0$. Thus, if there is some J_ℓ that has distinct eigenvalues, then all of the J_i must be diagonalizable, which we have assumed is not the case. Thus, each J_i must have only one eigenvalue, call it λ_i. Note that since each J_i has entries in $\mathfrak{O}_K$ and a repeated eigenvalue λ_i, then for each i, we have that λ_i is the only root of a second degree monic polynomial with coefficients in $\mathfrak{O}_K$. Hence each λ_i is an algebraic integer, and moreover, it belongs to the field K; thus $\lambda_i \in \mathfrak{O}_K$ for each i. Now, if two invertible non-diagonalizable 2-by-2 matrices M and N commute, then any eigenvector for M must also be an eigenvector for N. Thus, there exists a change of basis matrix B with entries in K such that $B J_i B^{-1} = a_i \cdot \begin{pmatrix} 1 & c_i \\ 0 & 1 \end{pmatrix}$ for each i (where $a_i = \lambda_i \in \mathfrak{O}_K$ and $c_i \in K$). $\qquad\square$

Note that each a_i is nonzero since we assumed that each Φ_i is an isogeny (see Lemma 3.1).

Since we work in a two-dimensional space, the linear variety $\mathcal{V}$ from Proposition 4.1 is a line L through the origin (note that in Proposition 2.11 we already covered the case $\dim(V) = 0$, while the case $V = A^2$ is trivial). So, if we let $\begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix}$ for some constants $\delta_1, \delta_2 \in \mathbb{C}_p$, then Proposition 4.1 reduces the problem to determining for which tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ we have that

$$\prod_{i=1}^{r} a_i^{n_i} \cdot \begin{pmatrix} 1 & \sum_{i=1}^{r} n_i c_i \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix} \in v_0 + L.$$

So, there exist constants $\delta_3, \delta_4, \delta_5 \in \mathbb{C}_p$ such that the above equation reduces to

$$(5.4) \qquad \prod_{i=1}^{r} a_i^{n_i} \cdot \left(\delta_3 \cdot \left(\delta_1 + \delta_2 \cdot \left(\sum_{i=1}^{r} n_i c_i \right) \right) + \delta_4 \cdot \delta_2 \right) = \delta_5.$$

After collecting the terms, and introducing new constants $A, B \in \mathbb{C}_p$, we conclude that the equation (5.4) reduces to either

$$(5.5) \qquad \sum_{i=1}^{r} c_i n_i = B,$$

or

$$(5.6) \qquad \prod_{i=1}^{r} a_i^{n_i} = A,$$

or

$$(5.7) \qquad \prod_{i=1}^{r} a_i^{n_i} \cdot \left(A + \sum_{i=1}^{r} n_i c_i \right) = B.$$

It is immediate to see that the set E of solution tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ to equation (5.5) belongs to the class $\mathcal{C}$. Indeed, E is a finite union of cosets of $H \cap \mathbb{N}^r$, where $H \subset \mathbb{Z}^r$ is the subgroup consisting of all solutions $(n_1, \ldots, n_r) \in \mathbb{Z}^r$ to the equation $\sum_{i=1}^{r} c_i n_i = 0$; the cosets are translates of H by the minimal elements of E with respect to the usual order $\prec$ on $\mathbb{N}^r$ (see Proposition 2.3).

Either arguing directly (note that each $|a_i|^2 \in \mathbb{N}$ since a_i is a nonzero algebraic integer from a quadratic imaginary field), or alternatively using the proof of the Mordell-Lang Conjecture for the multiplicative group [12] we conclude that the set of tuples $(n_1, \ldots, n_r)$ which are solutions to equation (5.6) also belongs to the class $\mathcal{C}$.

Now, assume equation (5.4) reduces to (5.7). Also note that we may assume that $B \neq 0$ since otherwise we would have that $\sum_{i=1}^{r} c_i n_i = -A$ (note that each a_i is nonzero), which reduces everything to the equation (5.5) studied above.

We will show first that it is impossible that the set of values for $\prod_{i=1}^{r} a_i^{n_i}$ is infinite as $(n_1, \ldots, n_r)$ runs through the tuples of all solutions to equation (5.7). Indeed, if the set of values for $\prod_{i=1}^{r} a_i^{n_i}$ would be infinite, then we obtain that $A \in K$, and thus, that $B \in K$ (since $a_i \in \mathfrak{O}_K$ and $c_i \in K$ for each i). Furthermore, at the expense of replacing both A and B, but also the c_i's by integral multiples of them, we may even assume that $A, B \in \mathfrak{O}_K$ and also $c_i \in \mathfrak{O}_K$ for each i. Since $B \neq 0$, then $A + \sum_{i=1}^{r} c_i n_i \neq 0$. On the other hand, $A + \sum_{i=1}^{r} c_i n_i \in \mathfrak{O}_K$, and $\mathfrak{O}_K$ is the ring of integers in a quadratic imaginary field. Therefore, the absolute value $| A + \sum_{i=1}^{r} c_i n_i |$ is uniformly bounded away from 0; more precisely, $| A + \sum_{i=1}^{r} c_i n_i | \geq 1$. So, for each solution tuple $(n_1, \ldots, n_r)$ to (5.7), we have that $\prod_{i=1}^{r} |a_i|^{n_i} \leq |B|$. On the other hand, because $\mathfrak{O}_K$ is the ring of integers in a quadratic imaginary field, there are finitely many elements $D \in \mathfrak{O}_K$ such that $|D| \leq |B|$. This contradicts our assumption that the set of values for $\prod_{i=1}^{r} a_i^{n_i}$ is infinite.

Now, since there are only finitely many distinct values for $\prod_{i=1}^{r} a_i^{n_i}$ as $(n_1, \ldots, n_r)$ runs over all tuples which are solutions to equation (5.7), then (5.7) reduces to solving simultaneously finitely many pairs of equations of the form $\prod_{i=1}^{r} a_i^{n_i} = D$ and $\sum_{i=1}^{r} c_i n_i = -A + B/D$ for some numbers D belonging to a finite set. However, the solutions set of tuples $(n_1, \ldots, n_r) \in \mathbb{N}^r$ to either one of the above equations belongs to the class $\mathcal{C}$ (as we argued

before for equations (5.5) and (5.6)). Since the class $\mathcal{C}$ is closed under intersections (see Proposition 2.6), we are done.

6. Counterexamples

In this section we give two examples in which Question 1.2 has a negative answer. Both examples involve two algebraic group endomorphisms of $\mathbb{G}_m^3$. In the first example, the subvariety V is a line which is a coset of a one-dimensional algebraic subgroup of $\mathbb{G}_m^3$. In this example the endomorphisms are in fact automorphisms. In the second example, the subvariety V is a two-dimensional algebraic subgroup of $\mathbb{G}_m^3$, and the algebraic group endomorphisms do not induce automorphisms on any positive-dimensional subvariety of $\mathbb{G}_m^3$ (see Lemma 6.1).

6.1. An example where V is a line. Let Φ and Ψ be the endomorphisms of $\mathbb{G}_m^3$ given by

$$\Phi(x,y,z) = \left(xy^{-1},\, yz^{-2},\, z\right) \quad \text{and} \quad \Psi(x,y,z) = \left(xy^2,\, yz^4,\, z\right).$$

Then $\Phi\Psi(x,y,z) = \Psi\Phi(x,y,z) = (xyz^{-4},\, yz^2,\, z)$. Moreover, for any $m,n \in \mathbb{N}$ we have

$$\Phi^m\Psi^n(x,y,z) = \left(xy^{2n-m}z^{4n(n-1)-4mn+m(m-1)},\, yz^{4n-2m},\, z\right).$$

Let V be the subvariety $\{(2,y,3) : y \in \mathbb{C}\}$ of $\mathbb{G}_m^3$, and let $\alpha := (2,9,3)$. Then, for $m,n \in \mathbb{N}$, the point $\Phi^m\Psi^n(\alpha)$ lies in $V(\mathbb{C})$ if and only if

$$2(2n - m) + 4n(n - 1) - 4mn + m(m - 1) = 0,$$

or, in other words, $(2n - m)^2 = 3m$. The solutions of this last equation in nonnegative integers are visibly $m = 3k^2$ and $n = 3(k^2 \pm k)/2$ with $k \in \mathbb{N}$. But the set $\{(3k^2, 3(k^2 \pm k)/2) : k \in \mathbb{N}\}$ is not in the class $\mathcal{C}$ (for instance, because there are arbitrarily large gaps between consecutive values of the first coordinate).

In this example, V is a line, and in fact is the translate of the one-dimensional algebraic subgroup $\{(1,y,1) : y \in \mathbb{C}\}$ by the point $(2,1,3)$. This example resembles previous counterexamples to our general Question 1.4, in that Φ and Ψ are automorphisms. Below we present another example which does not have this property.

6.2. An example involving non-automorphisms. Let Φ and Ψ be the endomorphisms of $\mathbb{G}_m^3$ given by

$$\Phi(x,y,z) = \left(x^2y^{-1},\, y^2z^{-2},\, z^2\right) \quad \text{and} \quad \Psi(x,y,z) = \left(x^2y^2,\, y^2z^4,\, z^2\right).$$

Then $\Phi\Psi(x,y,z) = \Psi\Phi(x,y,z) = \left(x^4y^2z^{-4},\, y^4z^4,\, z^4\right)$. Moreover, for any $m, n \in \mathbb{N}$ we have that $\Phi^m\Psi^n(x,y,z)$ equals

$$\left(x^{2^{m+n}}\, y^{n2^{m+n}-m2^{m+n-1}}\, z^{n(n-1)2^{m+n}+m(m-1)2^{m+n-2}-mn2^{m+n}},\right.$$

$$\left. y^{2^{m+n}}\, z^{n2^{m+n+1}-m2^{m+n}},\, z^{2^{m+n}}\right).$$

Let V be the subvariety of $\mathbb{G}_m^3$ defined by $x = 1$, and let $\alpha := (1, 1/3, 9)$. Then, for $m, n \in \mathbb{N}$, the point $\Phi^m\Psi^n(\alpha)$ lies in $V(\mathbb{C})$ if and only if

$$\left(\frac{1}{3}\right)^{n2^{m+n}-m2^{m+n-1}}\, 9^{n(n-1)2^{m+n}+m(m-1)2^{m+n-2}-mn2^{m+n}} = 1,$$

or in other words

$$2^{m+n-1}(-2n + m + 4n(n-1) + m(m-1) - 4mn) = 0.$$

This last equation is equivalent to $(2n - m)^2 = 6n$, whose solutions in nonnegative integers are visibly $n = 6k^2$ and $m = 12k^2 \pm 6k$ with $k \in \mathbb{N}$. But the set of solutions $\{(12k^2 \pm 6k,\, 6k^2) : k \in \mathbb{N}\}$ is not in $\mathcal{C}$ (for instance, because there are arbitrarily large gaps between consecutive values of the second coordinate).

This example differs from all previous counterexamples to the generalization of Question 1.2 in that the semigroup S generated by Φ and Ψ contains no nonidentity element having a degree-one restriction to some positive-dimensional subvariety of $\mathbb{G}_m^3$. The reason for this is that $\Phi^m\Psi^n$ has characteristic polynomial $(X - 2^{m+n})^3$ (see Lemma 6.1 for a more general result).

Lemma 6.1. *Let $g \in \mathbb{N}$, and let $\Phi \in \mathrm{End}(\mathbb{G}_m^g)$ be an algebraic group endomorphism whose Jacobian at the identity of $\mathbb{G}_m^g$ has all eigenvalues of absolute value larger than one. Then there is no positive-dimensional subvariety V of $\mathbb{G}_m^g$ such that Φ restricts to an automorphism of V.*

Proof. Assume there exists a positive-dimensional subvariety $V \subset \mathbb{G}_m^g$ such that Φ restricts to an automorphism of V. Let $\alpha \in V(\mathbb{C})$ be a nontorsion point of $\mathbb{G}_m^g$ (note that V is positive-dimensional, and thus not all its points are torsion). Because Φ restricts to an endomorphism of V, the Φ-orbit $\mathcal{O}_{\langle\Phi\rangle}(\alpha)$ of α is contained in V. Applying Lemma 2.13, there exists a finitely generated subgroup $\Gamma \subset \mathbb{G}_m^g(\mathbb{C})$ such that $\mathcal{O}_{\langle\Phi\rangle}(\alpha)$ is contained in Γ. Because $\mathcal{O}_{\langle\Phi\rangle}(\alpha)$ is an infinite set contained in the intersection $V(\mathbb{C})\cap\Gamma$, we obtain that the Zariski closure W of $V(\mathbb{C})\cap\Gamma$ is a positive-dimensional subvariety of V. Using Theorem 1.1, we conclude that W contains a translate of a positive-dimensional algebraic subgroup H of $\mathbb{G}_m^g$. Because Φ restricts to an automorphism of V, then it induces a degree-one map on H. Therefore, the Jacobian $J_{\Phi,H}$ of Φ at the identity of H (which is also the identity of $\mathbb{G}_m^g$) is an invertible matrix over $\mathbb{Z}$; however, this is contradicted by the

fact that all eigenvalues of $J_{\Phi,H}$ have absolute value larger than one (because they are among the eigenvalues for the Jacobian of Φ at the identity of $\mathbb{G}_m^g$). $\qquad\square$

Remark. Using the inverse of the p-adic exponential map (as in the proof of Theorem 1.3(a)) reduces the examples of 6.1 and 6.2 to simple linear algebra. Matrices that commute must share a common Jordan block decomposition, which is slightly weaker than being simultaneously diagonalizable. So, for example, applying the p-adic logarithmic map to the endomorphisms in 6.1 converts Φ into $\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$ and converts Ψ into $\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$. Note also that the above counterexamples can be also constructed for endomorphisms of E^3, where E is an elliptic curve, since the whole argument is at the level of linear algebra after applying the p-adic logarithmic maps.

References

[1] J. P. Bell, *A generalised Skolem–Mahler–Lech theorem for affine varieties.* J. London Math. Soc. (2) **73** (2006), 367–379; corrig. J. London Math. Soc. (2) **78** (2008), 267–272. arXiv: math/0501309.

[2] J. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell–Lang problem for ètale maps.* Amer. J. Math. **132** (2010), 1655–1675.

[3] R. L. Benedetto, D. Ghioca, T. J. Tucker and P. Kurlberg (with an Appendix by U. Zannier), *A case of the dynamical Mordell–Lang conjecture.* To appear in Math. Ann., arXiv: 0712.2344.

[4] N. Bourbaki, Lie Groups and Lie Algebras. Chapters 1–3, Springer–Verlag, Berlin, 1998.

[5] L. Denis, *Géométrie et suites récurrentes.* Bull. Soc. Math. France **122** (1994), 13–27.

[6] G. Faltings, *The general case of S. Lang's theorem.* In Barsotti symposium in Algebraic Geometry 175–182, Academic Press, San Diego, 1994.

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

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

[9] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Linear relations between polynomial orbits.* To appear in Duke Mat. J.

[10] S. Iitaka, *Logarithmic forms of algebraic varieties.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **23** (1976), 525–544.

[11] ———, *On logarithmic Kodaira dimension of algebraic varieties.* In Complex Analysis and Algebraic Geometry Iwanami Shoten, Tokyo (1977), 175–189.

[12] S. Lang, *Integral points on curves.* Publ. Math. IHES **6** (1960), 27–43.

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

[14] K. Mahler, *Eine arithmetische Eigenshaft der Taylor-Koeffizienten. rationaler Funktionen* Proc. Kon. Ned. Akad. Wetensch. **38** (1935), 50–60.

[15] M. McQuillan, *Division points on semi-abelian varieties.* Invent. Math. **120** (1995), 143–159.

[16] J. Milne, *Abelian varieties.* available at www.jmilne.org/math/index.html.

[17] T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen.* In Comptes rendus du 8e congrès des mathématiciens scandinaves (1935), 163–188.

[18] 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: dghioca@math.ubc.ca

Thomas Tucker
Department of Mathematics
University of Rochester
Rochester, NY 14627
USA
E-mail: ttucker@math.rochester.edu

Michael E. Zieve
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109
USA
E-mail: zieve@umich.edu