Bull. Aust. Math. Soc. **104** (2021), 381–390
doi:10.1017/S0004972721000083

A SPARSITY RESULT FOR THE DYNAMICAL MORDELL–LANG CONJECTURE IN POSITIVE CHARACTERISTIC

DRAGOS GHIOCA ✉, ALINA OSTAFE, SINA SALEH and IGOR E. SHPARLINSKI

(Received 4 January 2021; accepted 16 January 2021; first published online 23 February 2021)

Abstract

We prove a quantitative partial result in support of the dynamical Mordell–Lang conjecture (also known as the *DML conjecture*) in positive characteristic. More precisely, we show the following: given a field K of characteristic p, a semiabelian variety X defined over a finite subfield of K and endowed with a regular self-map $\Phi : X \longrightarrow X$ defined over K, a point $\alpha \in X(K)$ and a subvariety $V \subseteq X$, then the set of all nonnegative integers n such that $\Phi^n(\alpha) \in V(K)$ is a union of finitely many arithmetic progressions along with a subset S with the property that there exists a positive real number A (depending only on X, Φ, α and V) such that for each positive integer M,

$$\#\{n \in S\colon n \le M\} \le A \cdot (1 + \log M)^{\dim V}.$$

2020 *Mathematics subject classification*: primary 11B37; secondary 11G25, 37P55.

Keywords and phrases: dynamical Mordell–Lang conjecture, linear recurrence sequences.

1. Introduction

1.1. Notation. Throughout this paper, we let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ denote the set of nonnegative integers. As always in arithmetic dynamics, we denote by Φ^n the nth iterate of the self-map Φ acting on some ambient variety X. For each point x of X, we denote its orbit under Φ by

$$\mathcal{O}_\Phi(x) := \{\Phi^n(x)\colon n \in \mathbb{N}_0\}.$$

Also, for us, an arithmetic progression is a set $\{an + b\}_{n\in\mathbb{N}_0}$ for some $a, b \in \mathbb{N}_0$; in particular, we allow the possibility that $a = 0$, in which case the above set is a singleton.

1.2. The dynamical Mordell–Lang conjecture. The dynamical Mordell–Lang conjecture (see [7]) predicts that for an endomorphism Φ of a quasiprojective variety

D. Ghioca and S. Saleh were partially supported by a Discovery Grant from NSERC, A. Ostafe by ARC Grants DP180100201 and DP200100355, and I. Shparlinski by ARC Grant DP200100355.

X defined over a field K of characteristic 0, given a point $\alpha \in X(K)$ and a subvariety $V \subseteq X$, the set

$$\mathcal{S}(\Phi, \alpha; V) := \{n \in \mathbb{N}_0 \colon \Phi^n(\alpha) \in V(K)\} \tag{1.1}$$

is a finite union of arithmetic progressions; for a comprehensive discussion of the dynamical Mordell–Lang conjecture, we refer the reader to the book [2].

When the field K has positive characteristic, then under the same setting as above, the return set $\mathcal{S}$ from (1.1) is no longer a finite union of arithmetic progressions, as shown in [6, Examples 1.2 and 1.4]. Instead, the following conjecture is expected to hold.

Conjecture 1.1 (Dynamical Mordell–Lang conjecture in positive characteristic). Let X be a quasiprojective variety defined over a field K of characteristic p. Let $\alpha \in X(K)$, let $V \subseteq X$ be a subvariety defined over K and let $\Phi : X \longrightarrow X$ be an endomorphism defined over K. Then the set $\mathcal{S}(\Phi, \alpha; V)$ given by (1.1) is a union of finitely many arithmetic progressions along with finitely many sets of the form

$$\left\{ \sum_{j=1}^{m} c_j p^{a_j k_j} : k_j \in \mathbb{N}_0 \ \text{for each}\ j = 1, \ldots, m \right\} \tag{1.2}$$

for some given $m \in \mathbb{N}$, some given $c_j \in \mathbb{Q}$ and some given $a_j \in \mathbb{N}_0$. (Note that in (1.2), the parameters c_j and a_j are fixed, while the unknowns k_j vary over all nonnegative integers for $j = 1, \ldots, m$.)

In [3], Conjecture 1.1 is proven for regular self-maps Φ of tori assuming that one of the following two hypotheses is met:

(A) $\dim V \leq 2$; or
(B) $\Phi : \mathbb{G}_m^N \longrightarrow \mathbb{G}_m^N$ is a group endomorphism and there exists no nontrivial connected algebraic subgroup G of $\mathbb{G}_m^N$ such that an iterate of Φ induces an endomorphism of G that equals a power of the usual Frobenius.

The proof from [3] employs various techniques from Diophantine approximation (in characteristic 0), combinatorics over finite fields and specific tools akin to semiabelian varieties defined over finite fields; in particular, the deep results of Moosa and Scanlon [9] are essential in the proof. Actually, the dynamical Mordell–Lang conjecture in positive characteristic turns out to be even more difficult than the classical dynamical Mordell–Lang conjecture since even the case of group endomorphisms of $\mathbb{G}_m^N$ leads to deep Diophantine questions in *characteristic* 0, as shown in [3, Theorem 1.4]. More precisely, [3, Theorem 1.4] shows that solving Conjecture 1.1 just in the case of group endomorphisms of tori is *equivalent* with solving the following polynomial–exponential equation: given any linear recurrence sequence $\{u_n\}$, a power q of the prime number p and positive integers $c_1, \ldots, c_m$ such that

$$\sum_{i=1}^{m} c_i < \frac{q}{2},$$

https://doi.org/10.1017/S0004972721000083 Published online by Cambridge University Press

then one needs to determine the set of all $n \in \mathbb{N}_0$ for which we can find $k_1, \ldots, k_m \in \mathbb{N}_0$ such that

$$u_n = \sum_{i=1}^{m} c_i q^{k_i}. \tag{1.3}$$

Equation (1.3) remains unsolved for general sequences $\{u_n\}$ when $m > 2$. For more details about these Diophantine problems, see [4] and the references therein.

1.3. Statement of our results. Before stating our main result, we recall that a semiabelian variety is an extension of an abelian variety by an algebraic torus; for more details of semiabelian varieties, we refer the reader to [3, Section 2.1] and the references therein.

We prove the following result towards Conjecture 1.1.

THEOREM 1.2. *Let K be a field of characteristic p, let X be a semiabelian variety defined over a finite subfield of K and let Φ be a regular self-map of X defined over K. Let $V \subseteq X$ be a subvariety defined over K and let $\alpha \in X(K)$. Then the set $\mathcal{S}(\Phi, \alpha; V)$ defined by (1.1) is a union of finitely many arithmetic progressions along with a set $S \subseteq \mathbb{N}_0$ for which there exists a constant A depending only on X, Φ, α and V such that for all $M \in \mathbb{N}$,*

$$\#\{n \in S \colon n \leq M\} \leq A \cdot (1 + \log M)^{\dim V}. \tag{1.4}$$

Our result strengthens [1, Corollary 1.5] for the case of regular self-maps of semiabelian varieties defined over finite fields since in [1] it is shown that the set S (as in the conclusion of Theorem 1.2) is of Banach density zero; however, the methods from [1] cannot be used to obtain a sparseness result such as the one in (1.4).

We sketch briefly the plan for our paper. In Section 2 we introduce the technical ingredients regarding linear recurrence sequences which are used in our proofs. Then, in Section 3, we prove Theorem 1.2 by combining [3, Theorem 3.2] with [8, Théorème 6].

2. Technical background for our proofs

2.1. Linear recurrence sequences. The content of this section overlaps with [3, Section 2] (see also [6, Section 3]).

A *linear recurrence sequence* is a sequence $\{u_n\}_{n \in \mathbb{N}_0}$ over $\bar{\mathbb{Q}}$ with the property that there exists $m \in \mathbb{N}$ and there exist $c_0, \ldots, c_{m-1} \in \bar{\mathbb{Q}}$ such that for each $n \in \mathbb{N}_0$,

$$u_{n+m} + c_{m-1} u_{n+m-1} + \cdots + c_1 u_{n+1} + c_0 u_n = 0. \tag{2.1}$$

For more details regarding linear recurrence sequences, we refer the reader to [10]; however, we will gather in this section the most important notions which will be used in our proof of Theorem 1.2.

https://doi.org/10.1017/S0004972721000083 Published online by Cambridge University Press

The characteristic roots of a linear recurrence sequence as in (2.1) are the solutions of the equation

$$x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0 = 0. \tag{2.2}$$

We let r_i (for $1 \le i \le s$) be the (nonzero) roots of (2.2). (As explained in [3, Section 3], we can always reduce to the case $c_0 \neq 0$ at the expense of disregarding finitely many terms from our sequence.) Then there exist polynomials $Q_i(x) \in \bar{\mathbb{Q}}[x]$ such that for all $n \in \mathbb{N}_0$,

$$u_n = \sum_{i=1}^{s} Q_i(n) r_i^n. \tag{2.3}$$

It will be convenient for us later on in our proof of Theorem 1.2 to consider linear recurrence sequences which are given by a formula such as the one in (2.3) for which the following two properties hold:

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

Linear recurrence sequences given by (2.3) and satisfying properties (i) and (ii) are called *nondegenerate*. Given an arbitrary linear recurrence sequence, we can always split it into finitely many linear recurrence sequences which are all nondegenerate; moreover, we can achieve this by considering instead of one sequence $\{u_n\}_{n\in\mathbb{N}_0}$, finitely many sequences which are all of the form $\{u_{nM+\ell}\}_{n\in\mathbb{N}_0}$ for a given $M \in \mathbb{N}$ and for $\ell = 0, \ldots, M-1$. Indeed, assume that some r_i or some r_i/r_j is a root of unity, say of order M; then, for each $\ell = 0, \ldots, M-1$,

$$u_{nM+\ell} = \sum_{i=1}^{s} Q_i(nM+\ell) r_i^{\ell} (r_i^M)^n. \tag{2.4}$$

We can rewrite (2.4) for $u_{nM+\ell}$ by collecting the powers r_i^M which are equal to achieve a nondegenerate linear recurrence sequence $v_n := u_{nM+\ell}$.

2.2. F-arithmetic sequences. The content of this section overlaps with [3, Section 3]. (We also mention [5], which was the starting point that led to the constructions from [3].)

In this section, we fix some finite field $\mathbb{F}_q$ of characteristic p; also, we let X be a semiabelian variety defined over $\mathbb{F}_q$. We let F be the Frobenius endomorphism of X induced by the field automorphism $x \mapsto x^q$. We let $P_{\min,F} \in \mathbb{Z}[x]$ be the minimal (monic) polynomial for the Frobenius (as an endomorphism of X); then $P_{\min,F}$ has simple roots: $\lambda_1, \ldots, \lambda_\ell$. Moreover, each λ_j (for $j = 1, \ldots, \ell$) has absolute value equal to q or to $q^{1/2}$.

Let $\{u_n\}_{n\in\mathbb{N}_0}$ be a linear recurrence sequence over $\bar{\mathbb{Q}}$. Also, let $m \in \mathbb{N}_0$ and let $\{U_n^{(i)}\}_{n\in\mathbb{N}_0}$ (for $i = 1, \ldots, m$) be linear recurrence sequences over $\bar{\mathbb{Q}}$, each having simple characteristic roots, all of the form $\lambda_j^{a_i}$ for some $a_i \in \mathbb{N}$. With this notation for the linear recurrence sequences $\{u_n\}_{n\in\mathbb{N}_0}$ and $\{U_n^{(i)}\}_{n\in\mathbb{N}_0}$ for $i = 1, \ldots, m$, and given some $a, b \in \mathbb{N}_0$,

https://doi.org/10.1017/S0004972721000083 Published online by Cambridge University Press

an *F-arithmetic sequence* is the set of all n of the form $ak + b$ (for some $k \in \mathbb{N}_0$) for which there exist $k_1, \ldots, k_m \in \mathbb{N}_0$ such that

$$u_n = U_{k_1}^{(1)} + \cdots + U_{k_m}^{(m)}. \tag{2.5}$$

Using the fact that the characteristic roots of each $U^{(i)}$ are $\lambda_j^{a_i}$, (2.3) shows that (2.5) is equivalent with

$$u_n = \sum_{i=1}^{m} \sum_{j=1}^{\ell} c_{i,j} \lambda_j^{a_i k_i} \tag{2.6}$$

for some given $c_{i,j} \in \bar{\mathbb{Q}}$.

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

3. Proof of Theorem 1.2

3.1. Dynamical Mordell–Lang conjecture and linear recurrence sequences. We continue with the notation as in Section 2. Since X is defined over a finite field $\mathbb{F}_q$ of q elements of characteristic p, we let $F : X \longrightarrow X$ be the Frobenius endomorphism corresponding to $\mathbb{F}_q$. We let $P \in \mathbb{Z}[x]$ be the minimal polynomial with integer coefficients such that $P(F) = 0$ in $\mathrm{End}(X)$. According to [3, Section 2.1], P is a monic polynomial and it has simple roots $\lambda_1, \ldots, \lambda_\ell$, each one of them of absolute value equal to q or to $\sqrt{q}$.

From [3, Theorem 3.2], the set $\mathcal{S}(\Phi, \alpha; V)$ defined by (1.1) is a finite union of generalised F-arithmetic sequences, each of which is an intersection of finitely many F-arithmetic sequences. Using (2.6), each one of these F-arithmetic sequences consists of all nonnegative integers n belonging to a suitable arithmetic progression for which there exist $k_1, \ldots, k_m \in \mathbb{N}_0$ such that

$$u_n = \sum_{i=1}^{m} \sum_{j=1}^{\ell} c_{i,j} \lambda_j^{a_i k_i} \tag{3.1}$$

for some given linear recurrence sequence $\{u_n\}$ over $\bar{\mathbb{Q}}$, some given $m \in \mathbb{N}_0$, some given constants $c_{i,j} \in \bar{\mathbb{Q}}$ and some given $a_1, \ldots, a_m \in \mathbb{N}$. Applying Part (1) of [3, Theorem 3.2], we also see that $m \leq \dim V$. Furthermore, the linear recurrence sequence $\{u_n\}$ (and the λ_i) along with the constants $c_{i,j}$ and a_i depend solely on X, Φ, α and V.

At the expense of further refining to another arithmetic progression (as explained in Section 2), we may assume from now on that the linear recurrence sequence $\{u_n\}$ is nondegenerate. In addition, we know that the characteristic roots of $\{u_n\}$ are all algebraic integers (see Part (2) of [3, Theorem 3.2]) and further the characteristic roots of $\{u_n\}$ are either equal to 1 or equal to positive integer powers of the roots of the minimal polynomial of Φ inside $\mathrm{End}(X)$. For more details, see [3, Section 3]. So,

https://doi.org/10.1017/S0004972721000083 Published online by Cambridge University Press

using (2.3), (3.1) becomes

$$\sum_{r=1}^{s} Q_r(n)\mu_r^n = \sum_{i=1}^{m}\sum_{j=1}^{\ell} c_{i,j}\lambda_j^{a_i k_i}, \tag{3.2}$$

where $\mu_1, \ldots, \mu_s$ are the characteristic roots of the recurrence sequence $\{u_n\}$ and $Q_1, \ldots, Q_s \in \bar{\mathbb{Q}}[x]$. Hence, we are left with finding all $n \in \mathbb{N}_0$ satisfying (3.2) for some $k_1, \ldots, k_m \in \mathbb{N}_0$.

3.2. Reduction to the case $s = 1$. If each polynomial Q_r from (3.2) is constant, then the famous result of Laurent [8] solving the classical Mordell–Lang conjecture (inside an algebraic torus) provides the desired conclusion that the set of all $n \in \mathbb{N}_0$ satisfying an equation of the form (3.2) must be a finite union of arithmetic progressions. So, from now on, we assume that not all of the polynomials Q_r are constant.

Without loss of generality, we assume that Q_1 is a nonconstant polynomial. According to [8, Section 8, page 319] (see also [10, Theorem 7.1]), all but finitely many solutions to (3.2) are also solutions to a *subsum* derived from (3.2) which contains the term $Q_1(n)\mu_1^n$. More precisely, there exist a subset Σ_1 with $1 \in \Sigma_1 \subseteq \{1, \ldots, s\}$ and a subset $\Sigma_2 \subseteq \{1, \ldots, m\} \times \{1, \ldots, \ell\}$ such that we search for all $n \in \mathbb{N}_0$ with the property that there exist some $k_1, \ldots, k_m \in \mathbb{N}_0$ such that the following equation holds:

$$\sum_{r\in\Sigma_1} Q_r(n)\mu_r^n = \sum_{(i,j)\in\Sigma_2} c_{i,j}\lambda_j^{a_i k_i}. \tag{3.3}$$

Moreover, letting $\pi_1 : \{1, \ldots, m\} \times \{1, \ldots, \ell\} \longrightarrow \{1, \ldots, m\}$ be the projection on the first coordinate, we have $m_1 := \#(\pi_1(\Sigma_2))$; in particular, $m_1 \leq m$. Without loss of generality, we assume that $\pi_1(\Sigma_2) = \{1, \ldots, m_1\}$ (with the understanding that, *a priori*, m_1 could be equal to 0, even though we show next that this is not the case).

Using [8, Théorème 6], (3.3) has finitely many solutions unless the following subgroup $G_\Sigma \subseteq \mathbb{Z}^{1+m_1}$ is nontrivial. As described in [8, Section 8, page 320], the subgroup G_Σ consists of all tuples $(f_0, f_1, \ldots, f_{m_1})$ of integers with the property that

$$\mu_r^{f_0} = \lambda_j^{a_i f_i} \quad \text{for each } r \in \Sigma_1 \text{ and each } (i,j) \in \Sigma_2. \tag{3.4}$$

Since μ_{r_2}/μ_{r_1} is not a root of unity if $r_1 \neq r_2$, we conclude that if Σ_1 contains at least two elements (we already have by our assumption that $1 \in \Sigma_1$), then $f_0 = 0$ in (3.4). Indeed, if there exists some r with $1 \neq r \in \Sigma_1$, then $\mu_r^{f_0} = \mu_1^{f_0}$ yields $f_0 = 0$ because μ_r/μ_1 is not a root of unity. Furthermore, if $f_0 = 0$, then, from (3.4), each $f_i = 0$ (since each λ_j has an absolute value greater than 1 and $a_i \in \mathbb{N}$). So, if Σ_1 has more than one element, then the subgroup G_Σ is trivial. Therefore, in this case, [8, Théorème 6] yields that (3.3) (and, therefore, also (3.2)) has finitely many solutions, as desired.

3.3. Concluding the argument. Therefore, from now on, we may assume that Σ_1 has a single element, say, $\Sigma_1 = \{1\}$. In particular, this implies that Σ_2 cannot be the empty set. Indeed, otherwise (3.3) would simply read

$$Q_1(n)\mu_1^n = 0,$$

https://doi.org/10.1017/S0004972721000083 Published online by Cambridge University Press

which would only have finitely many solutions n (since $\mu_1 \neq 0$ and Q_1 is nonconstant). So, we see that indeed Σ_2 is nonempty, which also means that $1 \leq m_1 \leq m$.

We have two cases: either μ_1 equals 1 or not.

Case 1. $\mu_1 = 1$. Then (3.3) reads

$$Q_1(n) = \sum_{(i,j)\in\Sigma_2} c_{i,j}\lambda_j^{a_i k_i}. \tag{3.5}$$

For (3.5), the subgroup G_Σ defined above as in [8, Section 8, page 320] is the subgroup $\mathbb{Z} \times \{(0,\ldots,0)\} \subseteq \mathbb{Z}^{1+m_1}$ since each integer f_i from (3.4) must equal 0 for $i = 1,\ldots,m_1$ (note that $\mu_1 = 1$, while each λ_j is not a root of unity). According to [8, Théorème 6, part (b)], there exist positive constants A_1 and A_2 depending only on Q_1, the $c_{i,j}$ and the a_i, such that for any solution $(n, k_1,\ldots,k_{m_1})$ of (3.5),

$$\max\{|k_1|,\ldots,|k_{m_1}|\} \leq A_1 \log|n| + A_2. \tag{3.6}$$

So, for each nonnegative integer $n \leq M$ (for some given upper bound M) for which there exist integers k_i satisfying (3.5), we have $|k_i| \leq A_2 + A_1 \log M$. Letting

$$A_3 := (2 \cdot \max\{A_1, A_2\} + 1)^{m_1},$$

we have at most $A_3(1 + \log M)^{m_1}$ possible tuples $(k_1,\ldots,k_{m_1}) \in \mathbb{Z}^{m_1}$, which may correspond to some $n \in \{0,\ldots,M\}$ solving (3.5). Since Q_1 is a polynomial of degree $D \geq 1$, we conclude that the number of solutions $0 \leq n \leq M$ to (3.5) is bounded above by $D \cdot A_3(1 + \log M)^{m_1}$. Finally, recalling that $m_1 \leq m \leq \dim V$, we obtain the desired conclusion from (1.4).

Case 2. $\mu_1 \neq 1$. In this case, since we also know that any characteristic root μ_r of the linear recurrence sequence $\{u_n\}_{n\in\mathbb{N}_0}$ is either equal to 1 or not a root of unity, we conclude that μ_1 is not a root of unity.

Equation (3.3) reads now

$$Q_1(n)\mu_1^n = \sum_{(i,j)\in\Sigma_2} c_{i,j}\lambda_j^{a_i k_i}. \tag{3.7}$$

We analyse again the subgroup $G_\Sigma \subseteq \mathbb{Z}^{1+m_1}$ containing the tuples $(f_0, f_1,\ldots,f_{m_1})$ of integers satisfying (3.4), that is,

$$\mu_1^{f_0} = \lambda_j^{a_i f_i} \quad \text{for each } (i,j) \in \Sigma_2. \tag{3.8}$$

Because μ_1 is not a root of unity and also each λ_j is not a root of unity, while the a_i are positive integers, we conclude that a nontrivial tuple $(f_0, f_1,\ldots,f_{m_1})$ satisfying (3.8) must actually have each entry nonzero (that is, $f_i \neq 0$ for each $i = 0,\ldots,m_1$). We let b be the least common multiple of $f_1,\ldots,f_{m_1}$. Then there exists an algebraic number λ such that

$$\mu_1 = \lambda^b. \tag{3.9}$$

https://doi.org/10.1017/S0004972721000083 Published online by Cambridge University Press

Note that since μ_1 is not a root of unity, then also λ is not a root of unity. We also define the nonzero integers

$$b_i := \frac{f_0 \cdot b}{f_i} \quad \text{for } i = 1, \ldots, m_1.$$

From (3.8), whenever there is a pair $(i, j) \in \Sigma_2$, then there exist roots of unity $\zeta_{j,i}$ of order dividing f_i such that

$$\lambda_j^{a_i} = \zeta_{j,i} \cdot \lambda^{b_i}. \tag{3.10}$$

Combining (3.10), (3.9) and (3.7), we see that our goal is to find all $n \in \mathbb{N}_0$ for which there exist some $k_1, \ldots, k_m \in \mathbb{N}_0$ such that

$$Q_1(n)\lambda^{bn} = \sum_{(i,j)\in\Sigma_2} c_{i,j}\zeta_{j,i}^{k_i} \cdot \lambda^{b_i k_i}. \tag{3.11}$$

Since $\zeta_{j,i}^{f_i} = 1$, $\zeta_{j,i}^{b} = 1$ for each $(j, i) \in \Sigma_2$. We also define $B_i := b \cdot b_i$ for each $i = 1, \ldots, m_1$. Each integer k_i can be written as

$$k_i = bK_i + R_i, \tag{3.12}$$

where $K_i := \lfloor k_i/b \rfloor$, $i = 1, \ldots, m_1$. Thus, the integers R_i from (3.12) belong to the set $\{0, 1, \ldots, b-1\}$. So, for each choice of a tuple

$$(R_1, \ldots, R_{m_1}) \in \{0, \ldots, b-1\}^{m_1}, \tag{3.13}$$

working with integers k_i satisfying (3.12) for the given choice of R_i transforms (3.11) into an equation of the form

$$Q_1(n)\lambda^{bn} = \sum_{i=1}^{m_1} d_i \lambda^{B_i K_i} \tag{3.14}$$

for some algebraic numbers $d_1, \ldots, d_{m_1}$ depending only on b, the $c_{i,j}$, the $\zeta_{j,i}$, for $(i, j) \in \Sigma_2$, and the choice of the tuple from (3.13). Therefore, there exist at most b^m distinct equations such as the one from (3.14). For each one of these finitely many equations of the form (3.14), we want to find all integers $n \in \mathbb{N}_0$ for which there exist some $K_1, \ldots, K_m \in \mathbb{N}_0$ such that the corresponding equation (3.14) holds.

Dividing (3.14) by λ^{bn} yields

$$Q_1(n) = \sum_{i=1}^{m_1} d_i \lambda^{g_i} \tag{3.15}$$

for some integers g_i. Again applying [8, Théorème 6, part (b)] (see also (3.6)) yields immediately that any solution $(n, g_1, \ldots, g_{m_1})$ to (3.15) must satisfy the inequality

$$\max\{|g_1|, \ldots, |g_{m_1}|\} \le A_4 \log |n| + A_5$$

for some constants A_4 and A_5 depending only on the initial data in our problem (X, Φ, α and V). Exactly as in *Case 1*, we conclude that letting

$$A_6 := (2 \cdot \max\{A_4, A_5\} + 1)^{m_1},$$

https://doi.org/10.1017/S0004972721000083 Published online by Cambridge University Press

for any given upper bound $M \in \mathbb{N}$, we have at most $A_6(1+\log M)^{m_1}$ possible tuples $(g_1,\ldots,g_{m_1}) \in \mathbb{Z}^{m_1}$, which may correspond to some $n \in \{0,\ldots,M\}$ solving (3.15). Since Q_1 is a polynomial of degree $D \geq 1$, we conclude that the number of solutions $0 \leq n \leq M$ to (3.15) is bounded above by $D \cdot A_6(1+\log M)^{m_1}$. Finally, recalling that $m_1 \leq m \leq \dim V$, we obtain the desired conclusion from (1.4).

This concludes our proof of Theorem 1.2.

4. Comments

REMARK 4.1. If in (3.2) there exists at least one characteristic root μ_r of $\{u_n\}$ which is multiplicatively independent with respect to each one of the λ_j, then there is never a subsum (3.3) containing μ_r on its left-hand side for which the corresponding group G_Σ would be nontrivial. So, in this case, (3.2) would have only finitely many solutions. Now, as proven in [3, Section 3], if Φ is a group endomorphism of the semiabelian variety X, then the characteristic roots μ_r are also characteristic roots of the minimal polynomial (in $\mathrm{End}(X)$) of Φ. Therefore, with the notation as in Theorem 1.2, arguing as in the proof of [3, Theorem 1.3], one concludes that if Φ is a group endomorphism of the semiabelian variety X with the property that each characteristic root of its minimal polynomial (in $\mathrm{End}(X)$) is multiplicatively independent with respect to each eigenvalue λ_j of the Frobenius endomorphism of X, then, for each $\alpha \in X(K)$, the set $\mathcal{S}(\Phi,\alpha;V)$ defined by (1.1) is a finite union of arithmetic progressions.

REMARK 4.2. In (3.15), if we deal with a polynomial Q_1 of degree 1, then the conclusion from (1.4) is sharp. More precisely, as a specific example, consider

$$Q_1(n) = n, \quad m_1 = m, \quad c_1 = \cdots = c_m = 1 \quad \text{and} \quad \lambda = p. \tag{4.1}$$

Then (3.15) reduces to the equation

$$n = \sum_{i=1}^{m} p^{k_i}.$$

The number of positive integers $n \leq M$ which have precisely m nonzero digits (all equal to 1) in base p is of the order of $(\log M)^m$, which shows that Theorem 1.2 is tight if the dynamical Mordell–Lang conjecture reduces to solving (3.15) given by (4.1). As proven in [3, Theorem 1.4], there are instances when the dynamical Mordell–Lang conjecture reduces *precisely* to such an equation.

For higher degree polynomials $Q_1 \in \mathbb{Z}[x]$ appearing in (3.15), one expects a lower exponent than m appearing in the upper bounds from (1.4). One also notices that for any polynomial Q_1, arguments n with k nonzero digits in base p lead to sparse outputs. Hence, simple combinatorics allows us to obtain a lower bound on the best possible exponent in (1.4). However, finding a more precise exponent replacing m in (1.4) when $\deg Q_1 > 1$ seems very difficult beyond some special cases. The authors hope to return to this problem in a subsequent paper.

Acknowledgement

The authors are very grateful to the referee for useful comments and suggestions.

References

[1] J. P. Bell, D. Ghioca and T. J. Tucker, 'The dynamical Mordell–Lang problem for Noetherian spaces', *Funct. Approx. Comment. Math.* **53** (2015), 313–328.

[2] J. P. Bell, D. Ghioca and T. J. Tucker, *The Dynamical Mordell–Lang Conjecture*, Mathematical Surveys and Monographs, 210 (American Mathematical Society, Providence, RI, 2016).

[3] P. Corvaja, D. Ghioca, T. Scanlon and U. Zannier, 'The dynamical Mordell–Lang conjecture for endomorphisms of semiabelian varieties defined over fields of positive characteristic', *J. Inst. Math. Jussieu*, to appear.

[4] P. Corvaja and U. Zannier, 'Finiteness of odd perfect powers with four nonzero binary digits', *Ann. Inst. Fourier (Grenoble)* **63** (2013), 715–731.

[5] D. Ghioca, 'The isotrivial case in the Mordell–Lang theorem', *Trans. Amer. Math. Soc.* **360**(7) (2008), 3839–3856.

[6] D. Ghioca, 'The dynamical Mordell–Lang conjecture in positive characteristic', *Trans. Amer. Math. Soc.* **371**(2) (2019), 1151–1167.

[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] M. Laurent, 'Équations diophantiennes exponentielles', *Invent. Math.* **78** (1984), 299–327.

[9] R. Moosa and T. Scanlon, 'F-structures and integral points on semiabelian varieties over finite fields', *Amer. J. Math.* **126** (2004), 473–522.

[10] W. Schmidt, 'Linear recurrence sequences', *Diophantine Approximation (Cetraro, Italy, 2000)*, Lecture Notes in Mathematics, 1819 (Springer, Berlin, Heidelberg, 2003), 171–247.

DRAGOS GHIOCA, Department of Mathematics,
University of British Columbia,
Vancouver, BC V6T 1Z2, Canada
e-mail: dghioca@math.ubc.ca

ALINA OSTAFE, School of Mathematics and Statistics,
University of New South Wales,
Sydney, NSW 2052, Australia
e-mail: alina.ostafe@unsw.edu.au

SINA SALEH, Department of Mathematics,
University of British Columbia,
Vancouver, BC V6T 1Z2, Canada
e-mail: sinas@math.ubc.ca

IGOR E. SHPARLINSKI, School of Mathematics and Statistics,
University of New South Wales,
Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au