THE MORDELL-LANG CONJECTURE IN POSITIVE CHARACTERISTIC REVISITED

RAHIM MOOSA AND THOMAS SCANLON

Abstract. We prove versions of the Mordell-Lang conjecture for semiabelian varieties defined over fields of positive characteristic.

Introduction

Faltings proved the Mordell-Lang conjecture (itself a generalization of the Mordell conjecture) in the following form [1].

Theorem 0.1 (Faltings)**.** *Let G be a semiabelian variety defined over the field of complex numbers $\mathbb{C}$. Let $X \subseteq G$ be a closed subvariety and $\Gamma \leq G(\mathbb{C})$ a finitely generated subgroup of the group of $\mathbb{C}$-points on G. Then $X(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ.*

Theorem 0.1 has been generalized in various ways. The reader may consult [4] for a discussion of the history of this problem and some of its generalizations. In attempting to generalize the Mordell-Lang conjecture to positive characteristic one encounters obstructions in even the simplest cases.

Let $K = \mathbb{F}_p(t)$ be the field of rational functions over the field of size p. Consider the square of the multiplicative group $G := \mathbb{G}_m^2$ regarded as the complement of the coordinate axes in the plane, X the subvariety defined by $x + y = 1$, and Γ the subgroup of $G(K)$ generated by $(t, 1-t)$. One checks easily that $X(K) \cap \Gamma = \{(t^{p^m}, 1 - t^{p^m}) : m \in \mathbb{N}\}$. Visibly, this set cannot be expressed as a finite union of cosets of subgroups of Γ.

Hrushovski salvaged a version of the Mordell-Lang conjecture in positive characteristic by treating varieties defined over finite fields as exceptional [2]. The present authors proved a version of the Mordell-Lang conjecture for semiabelian varieties defined over finite fields in [5]. Moreover, they extracted the model theoretic content of this version of the Mordell-Lang conjecture in analogy to Pillay's analysis of Theorem 0.1. That is, the original Mordell-Lang conjecture may be rephrased as *if G is a semiabelian variety defined over $\mathbb{C}$ and $\Gamma \leq G(\mathbb{C})$ is a finitely generated subgroup of its $\mathbb{C}$-points, then the induced structure on Γ is stable and weakly normal.* The bulk of the work in [5] is directed at a quantifier elimination theorem for the induced structure on the R-rational points of semiabelian schemes over finite fields where R is a finitely generated domain extending the field of definition.

In this current paper we survey the methods and results of [5] while extending those results to giving, among other results, an *absolute* version of the Mordell-Lang conjecture in positive characteristic.

Date: Jan. 21, 2003.

Thomas Scanlon was partially supported by NSF grant DMS-00071890.

The structure of this paper is as follows. In Section 1 we survey the main methods and results of [5]. In Section 2 we prove a version of the Mordell-Lang conjecture for groups of the form $G(R)$ where G is a semiabelian variety over a finite field $\mathbb{F}_q$ and R is the ring of regular functions of some irreducible affine variety over $\mathbb{F}_q^{alg}$. While the group $G(R)$ is not finitely generated, the methods of [5] apply directly to this problem. In Section 3 we prove an absolute version of the Mordell-Lang conjecture.

We thank Luc Bélair for inviting us to write this paper for these proceedings. We are grateful to the organizers (especially Paola D'Aquino) of the Ravello Euroconference on Model Theory for putting together and running such a wonderful meeting. The second author thanks Dragos Ghioca for discussing some problems related to this paper. As mentioned below, some extensions of theorems proved here will appear in Ghioca's thesis.

1. F-sets and varieties defined over finite fields

The counter-example to an immediate translation of the Mordell-Lang conjecture to positive characteristic described in the introduction comes close to being paradigmatic. Frobenius orbits give the primary obstruction to finiteness while sums of such orbits and sums with groups give the others.

Let us consider a few examples before delving into a technical discussion. Before we can say much about these examples, we need to recall the notion of a Frobenius morphism.

Let $k = \mathbb{F}_q$ be the field of q elements. If R is any k-algebra, then the function $\tau_q : R \to R$ defined by $x \mapsto x^q$ is a morphism of k-algebras which we call the *q-power Frobenus* or just the *Frobenius* if q is clear from the context. If K is an algebraically closed field extending k and $X \subseteq \mathbb{A}^n$ is an affine variety over K, then $X^{(q)}$ is the Zariski closure of the set $\{(a_1^q, \dots, a_n^q) : (a_1, \dots, a_n) \in X(K)\}$, and the q-power Frobenius defined co-ordinatewise on $\mathbb{A}^n$ maps $X(R)$ to $X^{(q)}(R)$. Visibly, the function $(x_1, \dots, x_n) \mapsto (x_1^q, \dots, x_n^q)$ is a regular morphism of algebraic varieties. We denote the induced morphism on X by $F : X \to X^{(q)}$ and refer to F as the *Frobenius morphism of X induced by the the q-power Frobenius.* This construction can be carried out in a co-ordinate free manner that extends to arbitrary algebraic varieties (not just affine ones). Moreover, it is not hard to see that if G is an algebraic group, then the Frobenius morphism $F : G \to G^{(q)}$ is a morphism of algebraic groups.

Notice that if X is defined over $k = \mathbb{F}_q$, then $X^{(q)} = X$ and F is a morphism from X to itself. We shall use this construction mostly in the case of G a commutative algebraic group over k.

Example 1.1. Let C be a smooth curve of genus at least three over a finite field $k = \mathbb{F}_q$. We consider C as a subvariety of its Jacobian J_C embedded via a k-rational cycle. Let $F : J_C \to J_C$ be the Frobenius morphism coming from the q-power Frobenius. Let $K := k(C)$ be the function field of C and set $\Gamma := J_C(K)$. The automorphism group of C is finite and we have

$$C(K^{\text{alg}}) \cap \Gamma = C(K) = C(k) \cup \{F^n\gamma : n \in \mathbb{N}, \gamma \in \text{Aut}(C)\}.$$

This set is a union of finitely many Frobenius orbits. Now consider $X := C + C$. Visibly, we have $X(K^{\text{alg}}) \cap \Gamma = X(K)$ contains

$$\{a + F^n\gamma : a \in C(k), \gamma \in \text{Aut}(C), n \in \mathbb{N}\} \cup \{F^m\gamma + F^n\delta : \gamma, \delta \in \text{Aut}(C), m, n \in \mathbb{N}\}.$$

If we choose C so the summation map $C \times C \to C + C$ is an isomorphism, then this containment can be replaced by an equality. Finally, to obtain the most general example we should take a sum with a group. For instance, we could think of J_C as an algebraic subgroup of $J_C \times J_C$ via $x \mapsto (x, 0)$. If we set $Y := X + (0 \times J_C)$, then $Y(K) = X(K) + (0 \times J_C)(K)$.

In order to give a precise statement about the induced structure on the groups of integral points on semiabelian schemes over finite fields, we abstract from this geometric context to a certain general class of modules

Definition 1.2. A *Frobenius ring* is a commutative ring $\mathbb{Z}[F]$ satisfying the following conditions.

- As the notation suggests, $\mathbb{Z}[F]$ is a simple extension of the ring of integers generated by a distinguished element F.
- $\mathbb{Z}[F]$ is a finite integral extension of $\mathbb{Z}$.
- F is not a zero divisor in $\mathbb{Z}[F]$.
- The ideal $F^\infty \mathbb{Z}[F] := \bigcap\limits_{n \geq 0} F^n \mathbb{Z}[F]$ is trivial.

These conditions hold for our intended example: take G a semiabelian variety over a finite field with $F : G \to G$ the corresponding Frobenius morphism. The ring $\mathbb{Z}[F]$ is then the subring of the endomorphism ring of G generated by F.

From now on, when we write $\mathbb{Z}[F]$ we mean that this ring is a Frobenius ring. With the definition of a Frobenius ring in place we may define F-sets.

Definition 1.3. If M is a $\mathbb{Z}[F]$-module, $a \in M$, and $\delta \in \mathbb{Z}_+$ is a positive integer, then we denote the F^δ orbit of a by $S(a; \delta) := \{F^{\delta n} a : n \in \mathbb{N}\}$. If $a_1, \ldots, a_n \in M$ is a sequence of elements of M and $\delta_1, \ldots, \delta_n \in \mathbb{Z}_+$ is a sequence of positive integers of the same length, then we denote the sum of the F^{δ_i} orbits of the a_is by $S(\vec{a}; \vec{\delta}) := \sum_{i=1}^n S(a_i; \delta_i) = \{\sum_{i=1}^n F^{\delta_i m_i} a_i : (m_1, \ldots, m_n) \in \mathbb{N}^n\}$. A set of the form $b + S(\vec{a}; \vec{\delta}) + H$ with $b \in M$ and $H \leq M$ a $\mathbb{Z}[F^\ell]$-submodule of M for some ℓ is called a *cycle-free F-set*. If H is the trivial group, then we refer to such a set as a *groupless cycle-free F-set*.

Remark 1.4. Definition 1.3 differs from the definition of cycle-free F-set as used in [5] in three respects. First, in [5], M is taken to be finitely generated. Secondly, the groups H were required to be $\mathbb{Z}[F]$-modules rather than merely $\mathbb{Z}[F^\ell]$-modules for some ℓ. Thirdly, in [5] a finite union of cycle-free F-sets was considered to be a cycle-free F-set itself.

Note that if $\ell \in \mathbb{Z}_+$ is a positive integer, then any F^ℓ-set is automatically an F-set. Conversely, any F-set may be expressed as a finite union of F^ℓ-sets.

With these definitions in place we can state a version of the main Mordell-Lang theorem of [5].

Theorem 1.5. *Let G be a semiabelian variety defined over a finite field, $F : G \to G$ the corresponding Frobenius morphism, and K an algebraically closed field extending the field of definition of G. If $\Gamma \leq G(K)$ is a finitely generated $\mathbb{Z}[F]$-submodule of $G(K)$ and $X \subseteq G$ is a closed subvariety, then $X(K) \cap \Gamma$ is a finite union of (cycle-free) F-sets.*

Remark 1.6. Comparing the hypothesis of Theorem 1.5 with those of the Mordell-Lang statement for characteristic 0 (Theorem 0.1), notice that finitely generated subgroups have been replaced by finitely generated $\mathbb{Z}[F]$-submodules (that is, we require Γ to be closed under F). Nevertheless, some of the natural cases are included in this statement. For example, if $R/\mathbb{F}_q$ is a finitely generated domain, then $G(R)$ is closed under F, and our theorem does solve the problem of describing the R-rational points of subvarieties of semiabelian varieties over finite fields.

In the statement of Theorem 1.5 we have been a bit loose with the meaning of "F-set." In our definition of "F-set" we take parameters $b, a_1, \ldots, a_n$ from the module M. In Theorem 1.5 there are two reasonable interpretations of M: Γ and $G(K)$. The theorem is correct as written with $M = G(K)$, but it is false with Γ unless we drop the parenthetical "cycle-free" and give a more intrinsic notion of F-set. Before doing so we consider yet another example.

Example 1.7. Let C be a smooth curve of genus at least two defined over a finite field k, embedded in its Jacobian J_C and having a trivial automorphism group. Let $K := k(C)$ be the function field of C and let $\gamma \in C(K) \subseteq J_C(K)$ be the identity morphism of C thought of as an element of $J_C(K)$. Let $F : J_C \to J_C$ be the Frobenius morphism of J_C corresponding to k, $\gamma' := -\gamma + F\gamma \in J_C(K)$, $\Gamma := \mathbb{Z}[F]\gamma$ the $\mathbb{Z}[F]$-module generated by γ, and $\Gamma' := \mathbb{Z}[F]\gamma'$ the $\mathbb{Z}[F]$-module generated by γ'. Let $Y := C - \gamma$. It is an easy matter to see that $C(K) \cap \Gamma = S(\gamma; 1)$. Thus, $Y(K) \cap \Gamma = S(\gamma; 1) - \gamma$. However, $S(\gamma; 1) - \gamma = \{0\} \cup \{\sum_{i=0}^{n} F^i \gamma' : n \in \mathbb{N}\} \subseteq \Gamma'$ so that we have $Y(K) \cap \Gamma' = S(\gamma; 1) - \gamma$. The set on the righthand side of the equality may be expressed as a cycle-free F-set in the sense of Γ, but not in the sense of Γ'.

We refer to sets of the form appearing in the description of $Y(K) \cap \Gamma'$ as *cycles* and taking them as a the basis of our description of F-sets we obtain an intrinsic form of the induced structure. More precisely, we have the following definition.

Definition 1.8. If M is a $\mathbb{Z}[F]$-module, $a \in M$, and $\delta \in \mathbb{Z}_+$ is a positive integer, then the F^δ cycle of a is the set $C(a; \delta) := \{\sum_{i=0}^{n} F^{i\delta} a : i \in \mathbb{N}\}$. If $a_1, \ldots, a_m \in M$ is a sequence of elements of M and $\delta_1, \ldots, \delta_m \in \mathbb{Z}_+$ is a sequence of positive integers of the same length, then we denote the sum of the F^{δ_j} cycles of the a_js by $C(\vec{a}; \vec{\delta}) := \sum_{j=1}^{m} C(a_j; \delta_j) = \{\sum_{j=1}^{m} \sum_{i=0}^{n_j} F^{i\delta_j} a_j : (n_1, \ldots, n_m) \in \mathbb{N}^m\}$. An *$F$-set* in a $\mathbb{Z}[F]$-module M is a set of the form $b + C(\vec{a}; \vec{\delta}) + H$ where $b, a_1, \ldots, a_m \in M$ are elements of M and $H \leq M$ is a $\mathbb{Z}[F^\ell]$-submodule of M for some ℓ.

It turns out that every cycle-free F-set may be expressed as a finite union of F-sets (as defined with cycles in place of orbits). For the sake of illustration, we note that the single orbit $S(a; \delta)$ may be expressed as $\{a\} \cup a + C(F^\delta a - a; \delta) = (a + C(0; 1)) \cup (a + C(F^\delta a - a; \delta)$.Thus, we do not lose any structure by replacing orbits with cycles.

Moreover, if $X \subseteq M$ is an F-set in some module M, then there is an embedding of M into some other module M' so that X is a finite union of cycle-free F-sets in the sense of M'. In this case, it is a matter of reversing the operations of the previous paragraph. That is, if $F^\delta b - b = a$, then we may express $C(a; \delta)$ as $-b + S(F^\delta b; \delta)$. One checks (using properties of Frobenius rings) that if M' is the quotient of $M \oplus \mathbb{Z}[F]$ by the submodule generated by $(-a, F^\delta - 1)$, then there is a natural embedding of M into M' and one may take b to be the image of $(0, 1)$ in M'. In the case that M arises as a submodule of $G(K)$, the K-points of a semiabelian variety G over a finite field with K algebraically closed, then one can find $b \in G(K)$ as the map $(F - 1) : G(K) \to G(K)$ is an isogeny and therefore surjective.

If one passes from a module to an extension, then while the class of cycle-free sets might change, the class of finite unions of F-sets does not. That is, if $M \leq M'$ is an extension of $\mathbb{Z}[F]$-modules and $X \subseteq M$ is a subset of M which is an F-set in the sense of M', then X is already a union of F-set in the sense of M. So, to say that a set is a union of F-sets (in the sense of cycles) is the same as to say that it is a union of cycle-free F-sets in the sense of some extension module.

The conclusion of Theorem 1.5 should be that $X(K)\cap\Gamma$ is a finite union of F-sets. Our proof of Theorem 1.5 is (mostly) an exercise in elementary algebraic geometry. There is a point in the proof at which a detailed analysis of the combinatorics of F-sets plays a decisive rôle. We sketch the proof in a more general situation in Section 2. For the remainder of this section we discuss the combinatorics of F-sets and their consequences for the model theory of these structures.

Suppose $S := b + S(a_1, \dots, a_m; \delta_1, \dots, \delta_m)$ and $T := d + S(c_1, \dots, c_n; \gamma_1, \dots, \gamma_n)$ are two groupless cycle-free F-sets. How does one study their intersection? For simplicity let us consider the case when all the δ_i's and γ_j's are 1. Trivially, we can express $S \cap T$ as the set of all $b + F^{r_1}a_1 + \cdots + F^{r_m}a_m$ such that for some $s_1, \dots s_n$,

$$F^{r_1}a_1 + \cdots + F^{r_m}a_m + F^{s_1}(-c_1) + \cdots + F^{s_n}(-c_n) = d - b$$

We are thus lead to consider "logarithmic sets" of tuples of natural numbers.

Definition 1.9. Given $\overline{x} = (x_1, \dots, x_\ell) \in M^\ell$ and $Y \subseteq M$, we define

$$\log_{\overline{x}} Y := \{(r_1, \dots, r_\ell) \in \mathbb{N}^\ell : F^{r_1}x_1 + \cdots + F^{r_\ell}x_\ell \in Y\}$$

The logarithmic set $\log_{\overline{x}} Y$ describes the ways that elements of Y may be expressed as a sum of iterates of F applied to the x_i's.

Going in the other direction we have a notion of exponentiation as well.

Definition 1.10. Let $B \subseteq \mathbb{N}^\ell$ be a set of ℓ-tuples of natural numbers. We define

$$F^B := \{(F^{b_1}, \dots, F^{b_\ell}) \in \mathbb{Z}[F]^\ell : (b_1, \dots, b_\ell) \in B\}$$

If $\overline{x} = (x_1, \dots, x_\ell) \in M^\ell$, then

$$F^B\overline{x} := \{\sum_{i=1}^{\ell} F^{b_i}x_i : (b_1, \dots, b_\ell) \in B\}$$

The key technical observation in [5] is that

Fact 1.11. *If M is a $\mathbb{Z}[F]$-module, $\overline{x} \in M^\ell$, and $y \in M$, then there is a positive integer δ such that $\log_{\overline{x}}\{y\}$ is the projection of a positive quantifier-free definable set in the structure $(\mathbb{N}, 0, \sigma, P_\delta)$ on the natural numbers, where σ is the successor function and $P_\delta(x)$ is a predicate that is interpreted as $x \equiv 0 \bmod \delta$.*

Now a projection of a positive quantifier-free definable set in $(\mathbb{N}, 0, \sigma, P_\delta)$ is called *δ-closed* and is a finite union of sets of the form $\overline{t} + V$ where $\overline{t} \in \mathbb{N}^\ell$ and $V \subset \mathbb{N}^\ell$ is given by a conjunction of finitely many equations of the form $x \equiv q \bmod \delta$, for some $0 \leq q < \delta$; $x = \sigma^s(y)$, for some $s \in \mathbb{N}$; or $x = p$, for some $p \in \mathbb{N}$. Returning to our description of the intersection of cycle-free groupless F-sets S and T above, and using Fact 1.11, we see that there is a δ-closed set $B \subset \mathbb{N}^m$ such that

$$S \cap T = b + F^B\overline{a}$$

It is then not hard to see that $S \cap T$ is a finite union of cycle-free F-sets in M. Using this technique, one shows:

Fact 1.12. *Suppose M is a $\mathbb{Z}[F]$-module.*

(a) *An intersection of two groupless F-sets is a finite union of groupless F-sets. An intersection of two groupless cycle-free F-sets is a finite union of groupless cycle-free F-sets.*

(b) *If $N \leq M$ is a submodule and U is an F-set in M, then $U \cap N$ is a finite union of F-sets in N.*

The consequences of Fact 1.11 go far beyond an understanding intersections of F-sets. For example, given $\overline{a} = (a_1, \dots a_\ell) \in M^\ell$, we can define an equivalence relation, $\sim_{\overline{a}}$, on $\mathbb{N}^\ell$, by $\overline{r} \sim_{\overline{a}} \overline{s} \iff F^{r_1}a_1 + \cdots + F^{r_\ell}a_\ell = F^{s_1}a_1 + \cdots + F^{s_\ell}a_\ell$. It follows immediately from Fact 1.11 that $E_{\overline{a}}$ is a definable equivalence relation in $(\mathbb{N}, 0, \sigma, P_\delta)$ for some $\delta > 0$. In this way, one can study the cycle-free groupless F-sets that are based on $\overline{a}$ by considering sets interpretable in the structures $(\mathbb{N}, 0, \sigma, P_\delta)$.

These structures on $\mathbb{N}$, which are naturally bi-interpretable with $(\mathbb{N}, 0, \sigma)$ itself, are structurally extremely simple. For example, they are of Morley rank 1, admit elimination of quantifiers and weak elimination of imaginaries, have definable Skolem functions, and are of trivial geometry. Via the "logarithmic" equivalence relations described above, these properties impose heavy restrictions on the behaviour of F-sets.

Let us say a word about the combinatorics behind Fact 1.11. We reduce to the case that M is finitely generated by observing that the intersection must be contained in the $\mathbb{Z}[F]$-module generated by the groupless F-sets in question. Let $K = \bigcup_n \ker F^n$. As M is finitely generated, $K = \ker F^{N_1}$ for some $N_1 \geq 0$. It follows that F is injective on $F^\infty M := \bigcap_{n=0}^{\infty} F^n M$. A consequence of Nakayama's Lemma and the fact that $\mathbb{Z}[F]$ is a Frobenius ring is that $F^\infty M$ is a finite set. (In fact, this consequence was one of the motivating factors behind the definition of a Frobenius ring.) It follows that some positive power of F must fix $F^\infty M$ pointwise. The δ that appears in Fact 1.11 is this positive integer.

For each $i \geq 0$, let $M_i = K + F^i M$. These are the points that are F^i divisible modulo K. We obtain a filtration of M, and define M_ω to be the intersection of this descending chain of $\mathbb{Z}[F]$-submodules: $M_0 = M \geq M_1 \geq M_2 \geq \cdots \geq M_\omega = \bigcap_{n=0}^{\infty} M_n$. This in turn induces a valuation on M, $v \colon M \to \omega + 1$, given by $v(x) \geq n$ if and only if $x \in M_n$. Properties of the valuation are then used to describe the shape that the logarithmic sets can take.

This analysis leads to a quantifier elimination and stability theorem for $\mathbb{Z}[F]$-modules with F-sets.

Theorem 1.13 (Theorems 5.12 and 6.11 of [5])**.** *Let M be a $\mathbb{Z}[F]$-module. Consider M as a structure in the language $\mathcal{L}$ having a predicate for each F-set in each Cartesian power of M. Then, M admits elimination of quantifiers in $\mathcal{L}$ and is stable.*

Theorem 1.13 together with Theorem 1.5 implies the stability of the induced structure on a finitely generated submodule of a semiabelian variety defined over a finite field.

2. A geometric version

In this section we prove a geometric version of Theorem 1.5. This version generalizes our previous theorem, but the proof follows a similar scheme.

We consider the case of G a semiabelian variety defined over a finite field k, $F : G \to G$ the corresponding Frobenius morphism, $K \geq k$ an algebraically closed extension field of k, and $\Gamma = \Theta + G(k^{\mathrm{alg}})$ where $\Theta \leq G(K)$ is a finitely generated $\mathbb{Z}[F]$-module. We obtain an example of such a situation by taking R a finitely generated, integral, commutative k^{alg}-algebra and letting $\Gamma := G(R)$ be the group of R-points on G. By the Lang-Néron theorem, $\Gamma/G(k^{\mathrm{alg}})$ is a finitely generated group. Let $S \leq R$ be a finitely generated k-algebra such that $G(S)$ surjects onto $\Gamma/G(k^{\mathrm{alg}})$. Then $\Gamma = \Theta + G(k^{\mathrm{alg}})$ where $\Theta := G(S)$ is a finitely generated $\mathbb{Z}[F]$-module.

Of course, we cannot expect $X(K) \cap \Gamma$ to be a finite union of F-sets for $X \subseteq G$ a general algebraic subvariety. For example, if X is itself defined over a finite field, then $X(K) \cap \Gamma$ contains $X(k^{\mathrm{alg}})$. However, this is essentially the only extra complication.

Theorem 2.1. *If $X \subseteq G$ is a closed subvariety of G, then $X(K) \cap \Gamma$ is a finite union of sets of the form $S + Y(k^{\mathrm{alg}})$ where $S \subseteq \Gamma$ is an F-set and $Y \subseteq G$ is a closed subvariety over k^{alg}.*

Proof. We work by induction on $\dim X$. Replacing X with the Zariski closure of $X(K) \cap \Gamma$ we may assume that $X(K) \cap \Gamma$ is Zariski dense in X. Taking finite unions, we may assume that X is irreducible. Passing to a quotient, we may assume that the stabilizer of X is trivial.

Note that $G(k^{\mathrm{alg}}) = F^\infty \Gamma := \bigcap_{n \geq 0} F^n \Gamma$. It follows that the natural maps $\Theta/F^n\Theta \to \Gamma/F^n\Gamma$ are isomorphisms for every $n \in \mathbb{Z}_+$. From Lemma 7.5 of [5] it follows that $\Theta/F^n\Theta$ is finite for each $n \in \mathbb{Z}_+$ so that the same is true of $\Gamma/F^n\Gamma$.

We break into two cases. In the first case there is some n such that no coset of $F^n\Gamma$ in Γ is Zariski dense in X while in the second case for each $n \in \mathbb{Z}_+$ there is some $\gamma_n \in \Gamma$ with $\gamma_n + F^n\Gamma$ Zariski dense in X.

In the first case, let $A \subseteq \Gamma$ be a finite set of coset representatives for $F^n\Gamma$ in Γ. For each $a \in A$ let $Y_a := \overline{X(K) \cap (a + F^n\Gamma)}$. We have reduced to the case that $X(K) \cap \Gamma$ is Zariski dense in X so that

$$\begin{aligned} X &= \overline{X(K) \cap \Gamma} \\ &= \overline{\bigcup_{a \in A} X(K) \cap (a + F^n\Gamma)} \\ &= \bigcup_{a \in A} \overline{X(K) \cap (a + F^n\Gamma)} \\ &= \bigcup_{a \in A} Y_a \end{aligned}$$

As we are in the first case, we have that $\dim Y_a < \dim X$. As X is irreducible and A is finite, we have $X \neq \bigcup_{a \in A} Y_a$. This is a contradiction.

So, we must be in the second case.

Let L be the separable closure of a finitely generated extension of k^{alg} with $G(L) \geq \Gamma$. Let $\mathcal{U}$ be a nonprincipal ultrafilter on ω and $\gamma := [(\gamma_n)]_{\mathcal{U}}$ be the limit of $(\gamma_n)_{n \in \omega}$ with respect to $\mathcal{U}$. Let ${}^*L$ be the ultrapower of L with respect to $\mathcal{U}$, ${}^*K$ be the ultrapower of K, and ${}^*\Gamma$ be the ultrapower of Γ. Note that $F^{\infty}{}^*\Gamma \leq G(({}^*L)^{p^\infty})$.

To say that a particular type definable set (in some expansion of the language of rings) is Zariski dense in a variety is a type definable condition on the canonical parameter of the variety. Thus, $X({}^*K) \cap (\gamma + F^{\infty}{}^*\Gamma)$ is Zariski dense in X. That is, $X - \gamma$ meets $G(({}^*L)^{p^\infty})$ in a Zariski dense set. So $X - \gamma$ is defined over $({}^*L)^{p^\infty}$.

Building on work of Bouscaren and Poizat (the details are given in Proposition 7.7 of [5]) one shows that the pair of fields $({}^*K, {}^*L^{p^\infty})$ is an elementary extension of the pair (K, k^{alg}). Thus, we find $\gamma' \in G(K)$ with $X - \gamma'$ defined over k^{alg}.

Let Γ' be the module generated by Γ and γ'. If we show that $X(K) \cap \Gamma'$ has the correct form, then the result follows for $X(K) \cap \Gamma$. Indeed, suppose $X(K) \cap \Gamma' = \bigcup_i S_i + Y_i(k^{\mathrm{alg}})$, where $S_i \subseteq \Gamma'$ is an F-set and $Y_i \subseteq G$ is a subvariety over k^{alg}. Fix $i \leq \ell$ and notice that $S_i \cap \Gamma = \bigcup_j T_{i,j}$ for appropriate F-sets $T_{i,j} \subseteq \Gamma$ as the intersection of an F-set with a submodule is a union of F-sets. As $Y_i(k^{\mathrm{alg}}) \subseteq G(k^{\mathrm{alg}}) \leq \Gamma$ we have that $[S_i + Y_i(k^{\mathrm{alg}})] \cap \Gamma = (S_i \cap \Gamma) + Y_i(k^{\mathrm{alg}}) = \bigcup_j T_{i,j} + Y_i(k^{\mathrm{alg}})$. Thus, $X(K) \cap \Gamma = \bigcup_{i,j} T_{i,j} + Y_i(k^{\mathrm{alg}})$.

Thus, we may assume that $\Gamma = \Gamma'$. Replacing X with $X - \gamma'$ and F with some power of itself, we may assume that X is defined over k.

We note for the sequel that there is a natural number n such that if $a \in (\Gamma \setminus F\Gamma)$, then $X + a$ is not defined over L^{q^n}.The proof of this assertion is given during the course of the proof of Theorem 7.8 of [5] and follows along the lines of our reduction to the case that X is defined over k. It follows that if $a \in \Gamma \setminus F\Gamma$, then $\overline{(X + a)(K) \cap F^n\Gamma}$ is not equal to X and therefore has lower dimension. As $F^n\Gamma$ has finite index in $F\Gamma$, one obtains from this that $\overline{(X + a)(K) \cap F\Gamma}$ has lower dimension than X for all $a \in \Gamma \setminus F\Gamma$.

Let $A \subseteq \Gamma$ be a finite set of coset representatives for the *non-zero* cosets of $F\Gamma$ in Γ. Let $Z_a := \overline{(X - a)(K) \cap F\Gamma}$ as above.

By induction we have that

$$\begin{aligned} X(K) \cap (\Gamma \setminus F\Gamma) &= \bigcup_{a \in A} X(K) \cap (a + F\Gamma) \\ &= \bigcup_{a \in A} a + [(X - a)(K) \cap F\Gamma] \\ &= \bigcup_{a \in A} a + Z_a(K) \cap F\Gamma \\ &= \bigcup_{i=1}^{n} S_i + Y_i(k^{\mathrm{alg}}) \end{aligned}$$

where each S_i is an F-set and Z_i is an algebraic variety defined over k^{alg}. Let m be sufficiently divisible so that each Y_i is defined over the extension of k of degree m. We compute.

$$
\begin{aligned}
X(K) \cap (\Gamma \setminus F^{\infty}\Gamma) &= \bigcup_{t=0}^{\infty} X(K) \cap (F^{t}\Gamma \setminus F^{t+1}\Gamma) \\
&= \bigcup_{j=0}^{\infty} \bigcup_{\ell=0}^{m-1} X(K) \cap [F^{mj+\ell}\Gamma \setminus F^{mj+\ell+1}\Gamma] \\
&= \bigcup_{j=0}^{\infty} F^{mj}[\bigcup_{\ell=0}^{m-1} F^{\ell}(X(K) \cap (\Gamma \setminus F\Gamma))] \\
&= \bigcup_{j=0}^{\infty} F^{mj}[\bigcup_{\ell=0}^{m-1} \bigcup_{i=1}^{n} F^{\ell}S_i + Y_i^{(q^{\ell})}(k^{\mathrm{alg}})] \\
&= \bigcup_{\ell=0}^{m-1} \bigcup_{i=1}^{n} \bigcup_{j=0}^{\infty} F^{mj}(F^{\ell}S_i) + Y_i^{(q^{\ell})}(k^{\mathrm{alg}})
\end{aligned}
$$

By Corollary 7.3 of [5], the set $\bigcup_{j=0}^{\infty} F^{mj}(F^{\ell}S_i)$ is a subset of a finite union of F-sets that are themselves contained in X. Thus, $X(K) \cap [\Gamma \setminus F^{\infty}\Gamma]$ is a finite union of sets of the requisite form. As $F^{\infty}\Gamma = G(k^{\mathrm{alg}})$, we have $X(K) \cap F^{\infty}\Gamma = X(k^{\mathrm{alg}})$. This observation completes the proof. □

Further Extensions

Dragos Ghioca has extended this argument to some other cases. Ghioca has considered the case of t-adic closures of finitely generated groups. That is, if k is a finite field and G is a semiabelian variety over $k((t))$, then the group $G(k((t)))$ is naturally a topological group with the topology inherited from the t-adic topology on $k((t))$. If $\Gamma \leq G(k((t)))$ is a finitely generated group, then one can consider $\overline{\Gamma}$, the closure of Γ with respect to this topology. Ghioca has shown that when G is strongly isotrivial, $\Gamma \leq G(k(((t)))$ is a finitely generated $\mathbb{Z}[F]$-module, and $X \subseteq G$ is a closed subvariety, then $X(k((t))) \cap \overline{\Gamma}$ is a finite union of sets of the form $a + S + [H(k((t))) \cap \overline{\Gamma}]$ where S is a groupless F-set, a is a point, and $H \leq G$ is an algebraic subgroup.

Ghioca has also extended this study to purely inseparable extensions.

Theorem 2.2 (Ghioca)**.** *Let G be a semiabelian variety over a finite field $\mathbb{F}_q$ and let $F : G \to G$ be the corresponding Frobenius morphism. Let R be a finitely generated integral domain extending k. Let K be the algebraic closure of the fraction field of R and let $R' := \{x \in K : (\exists n \in \mathbb{Z}_+) x^{q^n} \in R\}$ be the perfect closure of R in K. [Note that $F : G(R') \to G(R')$ is an automorphism of this group.] Then, if $X \subseteq G$ is a subvariety of G the set $X(R')$ is a finite union of sets of the form $a + H(R') + \{\sum_{i=1}^{n} F^{\delta_i m_i} b_i : \vec{m} \in \mathbb{Z}^n\}$ for some $a, b_1, \ldots, b_n \in G(K)$, $\delta_1, \ldots, \delta_n \in \mathbb{Z}_+$, and $H \leq G$ an algebraic subgroup.*

Theorem 2.2 follows from the uniform version of Theorem 1.5. These results will appear as parts of Ghioca's doctoral dissertation.

3. Absolute Mordell-Lang

In the introduction we said that Hrushovski salvaged the Mordell-Lang conjecture in positive characteristic by treating the case of varieties defined over finite fields as exceptions [2]. It would be fairer to say that he reduced the general problem to the case of varieties defined over finite fields. Let us recall what Hrushovski actually showed. We begin by fixing some notation. Let p be a prime number, $k := \mathbb{F}_p^{\mathrm{alg}}$ be the algebraic closure of the prime field, and let K be any algebraically closed field extending k. If G is a semi-abelian variety over K, then a closed subvariety $X \subseteq G$ is said to be *special* if it is of the form $c + h^{-1}(X_\circ)$, where $c \in G(K)$, $h : G_1 \to G_\circ$ is a surjective morphism from an algebraic subgroup $G_1 \subset G$ to a group variety $G_\circ$ over k, and $X_\circ \subset G_\circ$ is a closed subvariety also over k. Note, for instance, that translates of algebraic subgroups of G are special in this sense. Hrushovski's theorem (restricted to the case of finitely generated subgroups of semiabelian varieties in characteristic p) then states:

Theorem 3.1 (Relative Mordell-Lang – Characteristic p)**.** *Suppose G is a semi-abelian variety over K, $X \subset G$ is a closed subvariety, and $\Gamma \leq G(K)$ is a finitely generated subgroup of the K-points. Then there are special closed subvarieties $X_1, \dots, X_\ell \subset X$ such that $X(K) \cap \Gamma = \bigcup_{i=1}^{\ell} X_i(K) \cap \Gamma$.*

It is instructive to consider what happens in two extreme cases. Suppose G is an abelian variety such that no subabelian variety of G admits a nontrivial map to an abelian variety over k. We say that G *is of k-trace zero*. It follows that the only special subvarieties of G are the translates of abelian subvarieties. Hence in this case Theorem 3.1 says that $X(K) \cap \Gamma$ is a finite union of cosets of Γ – that is, the conclusion of the characteristic 0 Mordell-Lang conjecture holds in charateristic p for abelian varieties of k-trace zero.

The other extreme case is when G is itself defined over k. In this case the theorem says that $X(K) \cap \Gamma$ is a finite union of sets of the form $X'(K) \cap \Gamma$ where X' is a translate of a subvariety of G over k. However, it does not describe what these latter intersections look like. This is the case we considered in [5] (and dicussed in Section 1 of the current paper); showing, under the additional assumption that Γ is closed under F, that $X(K) \cap \Gamma$ is a finite union of F-sets (Theorem 1.5).

For all intermediate cases, Hrushovski's theorem says (loosely speaking) that the failure of the conclusion of the characteristic 0 Mordell-Lang conjecture in characteristic p comes from semiabelian varieties over finite fields. This being the case, our results should give a general solution to the Mordell-Lang problem in positive characteristic. As there are several possible interpretations of the problem, we cannot rightly claim to have a complete solution. Nevertheless, in this section we describe one such solution.

To pass from the case of semiabelian varieties defined over a finite field to the general case, we must first consider *weakly isotrivial* varieties.

In what follows $k := \mathbb{F}_p^{\mathrm{alg}}$ is the algebraic closure of the prime field and $\mathbb{U}$ is an uncountable algebraically closed field of characteristic p. All varieties and morphisms, unless otherwise stated, will be defined over $\mathbb{U}$. All fields will be contained in $\mathbb{U}$. Also, *defined over* will be meant in the algebro-goemetric sense (as opposed to the model-theoretic sense). Moreover, we restict attention to the case of *abelian varieties.*

We begin with some generalities on the notion of isotriviality and trace.

Definition 3.2. Suppose X is a variety.

(a) X is *strongly isotrivial* if it is defined over k.
(b) X is *isotrivial* if there is a variety Y over k, and an isomorphism $f : Y \to X$.

(c) X is *weakly isotrivial* if there exists a variety Y over k, and a purely inseparable surjective morphism $f : Y \to X$.

Note that in both parts (b) and (c) of the definition, the morphism f need not be over the field of definition of X. That is, additional parameters may be required to witness (weak) isotriviality. Also, recall that at the level of $\mathbb{U}$-rational points, a purely inseparable morphism is just a morphism that is a bijection between its domain and its image.

Definition 3.3. Let K/k be any field extension, and G an abelian variety over K. A *K/k-trace of G* is a pair $(G_\circ, h)$ where $G_\circ$ is an abelian variety over k and $h : G_\circ \to G$ is a homomorphism over K with finite kernel; such that the following universal property holds:

Given any abelian variety G' over k and a homomorphism $h' : G' \to G$ over K, there exists a unique homorphism $g : G' \to G_\circ$ over k such that $h' = hg$.

Remark 3.4. As K/k is primary, a K/k-trace of G exists.[1] Moreover, by the universal property, if $(G'_\circ, h')$ is another K/k-trace of G then there is a (unique) isomorphism $g : G'_\circ \to G_\circ$ over k with $h' = hg$.

Lemma 3.5. *We follow the notation of Definition 3.3. That is K/k is an extension of fields and G is an abelian variety over K. Suppose G is weakly isotrivial, and let $(G_\circ, h)$ be a K^{sep}/k-trace of G. Then h is purely inseparable and surjective. In particular, there is a witness for the weak isotriviality of G over K^{sep}.*

Proof. By weak isotriviality, there is L/K^{sep} a finitely generated field extension, H an abelian variety over k, and $f : H \to G$ a purely inseparable surjective morphism over L. Translating by $-f(O_H) \in G(L)$, we may assume that f is a homomorphism of algebraic groups. Let $(G'_\circ, h')$ be any L/k-trace of G. By the universal property we have a homomorphism $g : H \to G'_\circ$ over k such that the following commutes:

$$\begin{array}{ccc} H & \xrightarrow{f} & G \\ {\scriptstyle g}\downarrow & \nearrow_{h'} & \\ G'_\circ & & \end{array}$$

As h' has finite kernel and f is a purely inseparable surjection, we obtain

$$\dim(G'_\circ) = \dim G = \dim H = \dim g(H).$$

Hence, $g(H) = G'_\circ$. It follows that h' is purely inseparable and surjective.

Now G is over K^{sep}, K^{sep} is a primary extension of k, and L is a primary extension of K^{sep}. Hence by VIII.3.7 of [3], $(G_\circ, h)$ is also an L/k-trace of G. By the above observation h is purely seperable and surjective. □

Until further notice, we fix G *a weakly isotrivial abelian variety, and K the minimal field of definition for G*. Note that $K/\mathbb{F}_p$ is finitely generated, and if G is strongly isotrivial then K is a finite field.

We wish to construct, in as canonical a manner as possible, an endomorphism of G that is "induced by the Frobenius automorphism of $\mathbb{U}$".

Definition 3.6. A *psuedo-Frobenius endomorphism of G*, $\widetilde{F} : G \to G$, is a purely inseparable surjective endomorphism over $K\mathbb{F}_q$ of the form hFh^{-1}, where

[1]See Lang [3].

- $(G_\circ, h)$ is a K^{sep}/k-trace of G;
- q is a power of p such that $G_\circ$ is over $\mathbb{F}_q$; and,
- $F : G_\circ \to G_\circ$ is the algebraic endomorphism induced by the q-power Frobenius map.

Lemma 3.7. *A psuedo-Frobenius endomorphism of G exists.*

Proof. Let $(G_\circ, h)$ be any K^{sep}/k-trace of G. As G is weakly isotrivial, Lemma 3.5 tells us that $h : G_\circ \to G$ is a purely inseperable surjective homomorphism over K^{sep}. Now let q be a power of p such that:

1. $G_\circ$ is over $\mathbb{F}_q$;
2. every algebraic automorphism of $G_\circ$ is over $\mathbb{F}_q$; and,
3. $h^{-1}[G(K^{\text{sep}})] \subset G_\circ((K^{\text{sep}})^{\frac{1}{q}})$.

That such a power of p exists follows from the following facts: $G_\circ$ is over $k = \mathbb{F}_p^{\text{alg}}$, every algebraic automorphism of $G_\circ$ is over k and the group of algebraic automorphisms of $G_\circ$ (which is the multpilicative group of units in the endomorphism ring of $G_\circ$) is finitely generated, and h is a purely inseperable isogeny over K^{sep}.

Let $F : G_\circ \to G_\circ$ be the algebraic endomorphism induced by the q-power Frobenius map $x \mapsto x^q$, and let $\widetilde{F} : G \to G$ be the definable endomorphism $\widetilde{F} := hFh^{-1}$. Note that $\widetilde{F}$ is a bijection (on the $\mathbb{U}$-rational points). It remains to show that $\widetilde{F}$ is an algebraic morphism, and that it is over $K\mathbb{F}_q$.

As $\widetilde{F}$ is a definable endomorphism, there exists $n \geq 0$ and an algebraic homomorphism $\hat{F} : G \to G^{p^n}$ such that the following commutes:

$$\begin{array}{ccc} G & \xrightarrow{\widetilde{F}} & G \\ & {\scriptstyle \hat{F}}\searrow \quad \swarrow{\scriptstyle F_G^n} & \\ & G^{(p^n)} & \end{array}$$

where F_G is the morphism on G induced by the Frobenius map. Choose n minimal with this property. We will show that $n = 0$ and hence $\hat{F} = \widetilde{F}$ is a morphism. First of all, if $x \in G(K^{\text{sep}})$ then $h^{-1}(x) \in G_\circ((K^{\text{sep}})^{\frac{1}{q}})$ (by our choice of q). Hence

$$\widetilde{F}(x) \in hF[G_\circ((K^{\text{sep}})^{\frac{1}{q}})] \subset h[G_\circ(K^{\text{sep}})] \subset G(K^{\text{sep}}).$$

We have shown that $\widetilde{F}[G(K^{\text{sep}})] \subset G(K^{\text{sep}})$. The above commuting diagram thus restricts to the following commuting diagram:

$$\begin{array}{ccc} G(K^{\text{sep}}) & \xrightarrow{\qquad \widetilde{F} \qquad} & G(K^{\text{sep}}) \\ & {\scriptstyle \hat{F}}\searrow \quad \swarrow{\scriptstyle F_G^n} & \\ & G^{(p^n)}((K^{\text{sep}})^{p^n}) & \end{array}$$

If $n > 0$ then $\hat{F} = F_G g$ for some algebraic homomorphism $g : G \to G^{(p^{n-1})}$, contradicting the minimal choice of n. Hence $n = 0$ and $\widetilde{F}$ is an algebraic morphism.

If $\Gamma(F) \subset G_\circ \times G_\circ$ is the graph of F, then $(h \times h)[\Gamma(F)(K^{\text{sep}})] \subset (G \times G)(K^{\text{sep}})$ is Zariski dense in the graph of $\widetilde{F}$, and hence $\widetilde{F}$ is over K^{sep}. It suffices, therefore, to show that $\widetilde{F}$ is model-theoretically definable over $K\mathbb{F}_q$. For this, it suffices to show that every automorphism of the universe which fixes $K\mathbb{F}_q$ pointwise fixes $\widetilde{F}$.

Let α be an automorphism of the universe which fixes $K\mathbb{F}_q$ pointwise. Then α fixes $G_\circ$ and G setwise, and

$$\widetilde{F}^\alpha = (hFh^{-1})^\alpha = \alpha hFh^{-1}\alpha^{-1} = (\alpha h\alpha^{-1})F(\alpha h\alpha^{-1})^{-1} = h^\alpha F(h^\alpha)^{-1},$$

where the penultimate equality is by the fact that α commutes with F (on $G_\circ$). Now $(G_\circ, h^\alpha)$ is another K^{sep}/k-trace of G. Hence, there is an algebraic automorphism g of $G_\circ$ over k, such that $h^\alpha = hg$. Moreover, by our choice of q, g is over $\mathbb{F}_q$. Hence $\widetilde{F}^\alpha = hgFg^{-1}h^{-1} = hFh^{-1} = \widetilde{F}$, where the penultimate equality is by the fact that F commutes with g. This proves the lemma. □

A psuedo-Frobenius endomorphism on a weakly isotrivial abelian variety is only unique up to iterations:

Lemma 3.8. *Suppose $\widetilde{F}' : G \to G$ is another psuedo-Frobenius endomorphism. Then for some $n, n' > 0$, $\widetilde{F}^n = (\widetilde{F}')^{n'}$.*

Proof. Let $(G_\circ', h'), q', F'$ be data that witnesses the psuedo-Frobenius nature of $\widetilde{F}'$ (see Definition 3.6). Note that $(G_\circ, h)$ and $(G_\circ', h')$ are both K^{sep}/k traces of G, and hence there is an isomorphism $g : G_\circ' \to G_\circ$ over k, with $h' = hg$. Let $N > 0$ be such that $\mathbb{F}_{p^N}$ contains $\mathbb{F}_q$ and $\mathbb{F}_{q'}$, and such that g is over $\mathbb{F}_{p^N}$. Let $n, n' > 0$ be such that $q^n = p^N = (q')^{n'}$. Then the p^N-power Frobenius automorphism induces F^n on $G_\circ$ and $(F')^{n'}$ on $G_\circ'$. Moreover, as g is over $\mathbb{F}_{p^N}$ and the p^N-power Frobenius automorphism fixes $\mathbb{F}_{p^N}$-pointwise, we have that $g(F')^{n'}g^{-1} = F^n$. Hence,

$$(\widetilde{F}')^{n'} = [h'F'(h')^{-1}]^{n'} = hg(F')^{n'}g^{-1}h^{-1} = hF^nh^{-1} = \widetilde{F}^n,$$

as desired. □

Recall from Definition 1.2 that a Frobenius ring is the abstract counterpart of the subring of the endomorphism ring of a strongly isotrivial semiabelian variety generated by a Frobenius.

Lemma 3.9. *If $\widetilde{F}$ is a psuedo-Frobenius endomorphism of G, then the subring of the endomorphism of G generated by $\widetilde{F}$, $R = \mathbb{Z}[\widetilde{F}]$, is a Frobenius ring.*

Proof. Let $R_\circ = \mathbb{Z}[F]$ be the subring of the endomorphism ring of $G_\circ$ generated by F. As $G_\circ$ is over $\mathbb{F}_q$ and F is induced by the q-power Frobenius, $R_\circ$ is a Frobenius ring. Hence it suffices to show that the map $\alpha : R_\circ \to R$ over $\mathbb{Z}$ induced by $F \mapsto \widetilde{F}$ is an isomorphism of R and $R_\circ$. But this map is just $P(F) \mapsto hP(F)h^{-1} = P(\widetilde{F})$. As h is bijective, α is an isomorphism of rings. □

Question 3.10. Suppose A is an abelian variety and $P : A \to A$ is a purely inseperable surjective endomorphism such that the subring of the endomorphism ring of A generated by P is a Frobenius ring. Does it follow that A is weakly isotrivial and αP is a psuedo-Frobenius endomorphism for some $\alpha \in \mathrm{Aut}(A)$?

In any case, from the strongly isotrivial case we deduce a version of the Mordell-Lang conjecture for weakly isotrivial groups.

Theorem 3.11 (Absolute Mordell-Lang – Weakly Isotrivial Case)**.** *Suppose G is a weakly isotrivial abelian variety and $\widetilde{F} : G \to G$ is a psuedo-Frobenius endomorphism. Suppose $\Gamma \leq G(\mathbb{U})$ is a finitely generated $\mathbb{Z}[\widetilde{F}]$-submodule. Then for $X \subset G$ a closed subvariety, $X(\mathbb{U}) \cap \Gamma$ is a finite union of $\widetilde{F}$-sets.*

Proof. Let $(G_\circ, h), q, F$ be data that witnesses the psuedo-Frobenius nature of $\widetilde{F}$. Let $R_\circ = \mathbb{Z}[F]$ be the subring of the endomorphism ring of $G_\circ$ generated by F. Let $\Gamma_\circ = h^{-1}(\Gamma) \leq G_\circ(\mathbb{U})$ and $X_\circ = h^{-1}(X) \subset G_\circ$. As $\widetilde{F} = hFh^{-1}$, $\Gamma_\circ$ is a finitely generated $R_\circ$-submodule of $G_\circ(\mathbb{U})$. Now h is a bijective group homomorphism from $G_\circ(\mathbb{U})$ to $G(\mathbb{U})$ that takes the action of F to the action of $\widetilde{F}$, and restricts to a bijection between $X_\circ(\mathbb{U}) \cap \Gamma_\circ$ and $X(\mathbb{U}) \cap \Gamma$. The theorem thus follows from Theorem 1.5 applied to $G_\circ, \Gamma_\circ, F, X_\circ$. □

A general case of the Mordell-Lang conjecture follows.

Theorem 3.12. *Let G be an abelian variety over $\mathbb{U}$, $X \subseteq G$ be a closed subvariety, and $\Gamma \leq G(\mathbb{U})$ a finitely generated subgroup. Let $G' \leq G$ be the maximal connected weakly isotrivial algebraic subgroup of G and set $\Gamma' := \Gamma \cap G'(\mathbb{U})$. We presume that Γ' is a $\mathbb{Z}[\widetilde{F}]$-submodule for some pseudo-Frobenius $\widetilde{F}$ on G'. Then $X(\mathbb{U}) \cap \Gamma$ is a finite union of sets of the form $a + S + (H(\mathbb{U}) \cap \Gamma)$ where $a \in G(\mathbb{U})$, $S \subseteq G'(\mathbb{U})$ is a groupless $\widetilde{F}$-set in G', and $H \leq G$ is an algebraic subgroup.*

Proof. We work by induction on $\dim X$. Taking finite unions, we may assume that X is irreducible. Passing to a quotient, we may assume that X has a trivial stabilizer. Replacing X with the Zariski closure of $X(\mathbb{U}) \cap \Gamma$, we may assume that $X(\mathbb{U}) \cap \Gamma$ is Zariski dense in X. By Hrushovski's theorem (3.1) there is a connected algebraic subgroup $G_1 \leq G$, an abelian variety $G_\circ$ defined over k, an algebraic variety $X_\circ \subseteq G_\circ$, and a surjective morphism of algebraic groups $h : G_1 \to G_\circ$ for which X is a translate of $h^{-1}X_\circ$. As X has no stabilizer, this morphism is necessarily a purely inseparable isogeny. Taking dual isogenies, it follows that G_1 is weakly isotrivial and is therefore a subgroup of G'. Hence $X \subseteq \alpha + G'$ for some $\alpha \in G(\mathbb{U})$. As the Γ points are dense in X, there is some $\gamma \in \Gamma$ for which $\gamma + X \subseteq G'$; and so $X(\mathbb{U}) \cap \Gamma = -\gamma + [(\gamma + X)(\mathbb{U}) \cap \Gamma] = -\gamma + [(\gamma + X)(\mathbb{U}) \cap \Gamma']$. We are now in the case of Theorem 3.11. □

Remark 3.13. Suppose K is a function field over which G, G', and $\widetilde{F}$ are defined. Then $\Gamma := G(K)$ satisfies the assumptions of Theorem 3.12.

References

[1] G. Faltings. The general case of S. Lang's conjecture. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 175–182. Academic Press, San Diego, CA, 1994.

[2] E. Hrushovski. The Mordell-Lang conjecture for function fields. *Journal of the American Mathematical Society*, 9(3):667–690, 1996.

[3] S. Lang. *Abelian Varieties*. Interscience Publishers, Inc., 1959.

[4] S. Lang. *Number theory. III*. Springer-Verlag, 1991.

[5] R. Moosa and T. Scanlon. F-structures and integral points on semiabelian varieties over finite fields. Preprint, 2002.

Massachusetts Institute of Technology, Department of Mathematics, 77 Mass. Ave., Cambridge, MA 02139-4307, USA

E-mail address: moosa@math.mit.edu

University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley, California 94720-3840, USA

E-mail address: scanlon@math.berkeley.edu