

DIVISION POINTS ON SUBVARIETIES OF ISOTRIVIAL SEMIABELIAN VARIETIES

DRAGOS GHIOCA AND RAHIM MOOSA

ABSTRACT. The positive characteristic function-field Mordell-Lang conjecture for finite rank subgroups is resolved for curves as well as for subvarieties of semiabelian varieties defined over finite fields. In the latter case, the structure of the division points on such subvarieties is determined.

1. INTRODUCTION

In its most general form, the Mordell-Lang theorem in characteristic 0 was proved by McQuillan [5] and states that if G is a semiabelian variety over \mathbb{C} , $\Lambda \leq G(\mathbb{C})$ is a finite rank subgroup, and $X \subset G$ is an irreducible subvariety whose intersection with Λ is Zariski dense, then X is a translate of an algebraic subgroup of G . (Recall that a subgroup is said to be of *finite rank* if it is contained in the divisible hull of a finitely generated subgroup.) This fails when \mathbb{C} is replaced by a field of positive characteristic. In [1], Abramovich and Voloch formulate and conjecture a function-field version of the Mordell-Lang statement in positive characteristic. The conjecture is proved, using model-theoretic techniques, by Hrushovski:

Theorem 1.1 (Mordell-Lang [3]). *Suppose L is an algebraically closed field of characteristic $p > 0$, G is a semiabelian variety defined over L , $X \subset G$ is an irreducible subvariety defined over L , and $\Lambda \leq G(L)$ is a subgroup of the prime-to- p divisible hull of a finitely generated subgroup of $G(L)$. If $X(L) \cap \Lambda$ is Zariski dense in X , then X is special. That is, $X = g + h^{-1}(X_0)$ where $g \in G(L)$, $h : G' \rightarrow G_0$ is a surjective homomorphism from an algebraic subgroup G' of G to a semiabelian variety G_0 defined over $\mathbb{F}_p^{\text{alg}}$, and X_0 is a subvariety of G_0 also defined over $\mathbb{F}_p^{\text{alg}}$.*

Besides the necessary modification of the conclusion from “translate of algebraic subgroup” to “special” (note that translates of algebraic subgroups are special), this theorem differs from the characteristic 0 version in that it only applies to subgroups of the *prime-to- p* divisible hull of a finitely generated group. Indeed, the more general statement is not accessible by the methods of [3] and remains open:

Conjecture 1.2 (Full Mordell-Lang). *Suppose $\Lambda \leq G(L)$ is a finite rank subgroup and $X \subset G$ is an irreducible subvariety. If $X(L) \cap \Lambda$ is Zariski dense in X , then X is special.*

Here is a summary of what we accomplish in this paper:

I. We reduce Conjecture 1.2 to the case of $\Lambda \leq G(K^{\text{per}})$ where K is a finitely generated field and $K^{\text{per}} := \{a \in K^{\text{alg}} \mid a^{p^n} \in K \text{ for some } n \in \mathbb{N}\}$ is the *perfect closure* of K . This is done in Section 2 by combining model theoretic methods of

Date: September 7, 2006.

Rahim Moosa was supported by an NSERC grant and a Waterloo start-up grant.

Scanlon [11] with an idea of Rössler's [10]. As a consequence, a result of Kim's [4] resolves the curve case of Conjecture 1.2.

II. We resolve Conjecture 1.2 for semiabelian varieties defined over finite fields. This is done in Section 3. Besides (I), we make use of a uniform description, obtained by Scanlon and the second author [8], of sets of the form $X(L) \cap \Gamma$ where Γ is a finitely generated subgroup of $G(L)$ that is invariant under the Frobenius endomorphism of G .

III. Still in the isotrivial case, we extend the results of [8] to give an explicit description of sets of the form $X(L) \cap \Gamma^{\text{div}}$ where Γ is a finitely generated subgroup of $G(L)$ that is invariant under the Frobenius endomorphism of G and $\Gamma^{\text{div}} := \{g \in G(L) \mid ng \in \Gamma \text{ for some } n \in \mathbb{Z}\}$ is the *divisible hull* of Γ . See Theorem 3.24 for a precise statement.

We are grateful to Thomas Scanlon for communicating to us Lemma 2.3 below.

We end this introduction with a slight elaboration on *special* subvarieties.

Definition 1.3. For $\Lambda \leq G(L)$, by a Λ -*special* subvariety of G we mean a subvariety of the form $g + h^{-1}(X_0)$ where $g \in \Lambda^{\text{div}}$, $h : G' \rightarrow G_0$ is a surjective homomorphism from an algebraic subgroup G' of G to a semiabelian variety G_0 defined over $\mathbb{F}_p^{\text{alg}}$, and X_0 is a subvariety of G_0 also defined over $\mathbb{F}_p^{\text{alg}}$.

If $\Lambda = \{0\}$ then we say *absolutely special* rather than $\{0\}$ -special.

A *special* subvariety is then a $G(L)$ -special subvariety (note that because L is algebraically closed $G(L)^{\text{div}} = G(L)$).

Fact 1.4. *An irreducible subvariety $X \subset G$ is absolutely special if and only if it has a Zariski dense set of torsion points.*

Proof. The right-to-left direction is the positive characteristic Manin-Mumford conjecture: see Pink and Rössler [9] for an algebraic proof, or Scanlon [11] for a model-theoretic proof that relies on the trichotomy theorem for generic difference fields in positive characteristic [2].

For the left-to-right direction, suppose $h : G' \rightarrow G_0$ is a surjective homomorphism where G' is an algebraic subgroup of G and G_0 is a semiabelian variety defined over $\mathbb{F}_p^{\text{alg}}$. Given $X_0 \subset G_0$ defined over $\mathbb{F}_p^{\text{alg}}$, it suffices to show that $h^{-1}(X_0)$ has a Zariski dense intersection with G'_{tor} . Since $X_0(\mathbb{F}_p^{\text{alg}})$ is Zariski dense in X_0 , this will follow once we observe that $h^{-1}(x)$ has a Zariski dense intersection with G'_{tor} for any $x \in X_0(\mathbb{F}_p^{\text{alg}})$. As taking the torsion subgroup is an exact functor on semiabelian varieties, $h(G'_{\text{tor}}) = (G_0)_{\text{tor}} = G(\mathbb{F}_p^{\text{alg}})$. It follows that for any $x \in X_0(\mathbb{F}_p^{\text{alg}})$, $h^{-1}(x) = g + \ker(h)$ for some $g \in G'_{\text{tor}}$. As every algebraic subgroup of G' has a Zariski dense set of torsion points, we have that $h^{-1}(x)$ has a Zariski dense intersection with G'_{tor} , as desired. \square

Corollary 1.5. (a) *The sum of (Λ) -special subvarieties is (Λ) -special.*

(b) *If G is defined over a finite field then a subvariety of X is special if and only if some translate of it is also defined over a finite field.*

Proof. It is clear from Fact 1.4 that the sum of absolutely special varieties is absolutely special. Part (a) follows as a Λ -special subvariety is of the form $g + Y$ where Y is absolutely special (and $g \in \Lambda^{\text{div}}$). Part (b) also follows from Fact 1.4 using the fact that if G is defined over $\mathbb{F}_p^{\text{alg}}$ then its torsion group is $G(\mathbb{F}_p^{\text{alg}})$. \square

2. TOWARD THE FULL MORDELL-LANG CONJECTURE IN POSITIVE CHARACTERISTIC

Fix L an algebraically closed field of positive characteristic p and G a semiabelian variety defined over L . All varieties in this section are assumed to be defined over L . Our aim here is to show that the following apparent weakening is in fact equivalent to the Full Mordell-Lang conjecture.

Conjecture 2.1. Let $K \leq L$ be a finitely generated field over which G is defined, $\Lambda \leq G(K^{\text{per}})$ a finite rank subgroup, and $X \subset G$ an irreducible subvariety defined over K . If $X(L) \cap \Lambda$ is Zariski dense in X , then X is special.

The published proof that Conjecture 2.1 implies Conjecture 1.2 (Theorem 4.3 of [11]) is incorrect; for one thing, it implicitly assumes that the semiabelian variety has $\mathbb{F}_p^{\text{alg}}$ -trace zero. We were unable to correct that argument. On the other hand, using some ideas from that argument together with a modification of a technique of Rössler's from [10] we are able to prove:

Theorem 2.2. *Conjecture 2.1 implies Conjecture 1.2.*

Proof. Let $\Lambda \leq \Gamma^{\text{div}}$ where $\Gamma \leq G(L)$ is a finitely generated group, and $X \subset G$ an irreducible subvariety such that $X(L) \cap \Lambda$ is Zariski dense in X . We wish to show that X is special. We proceed by induction on $\dim X$. Working modulo $\text{Stab}(X)$ we may assume that X has trivial stabiliser.

Let $K \leq L$ be a finitely generated field over which G and X are defined and such that $\Gamma \leq G(K)$. We begin with the following uniform version of the Manin-Mumford conjecture communicated to us by Thomas Scanlon.

Lemma 2.3 (T. Scanlon). *There exist absolutely special subvarieties Y_1, \dots, Y_ℓ of G such that for any $g \in \Gamma^{\text{div}}$ there is $I \subset \{1, \dots, \ell\}$ and $\zeta \in G_{\text{tor}}$ such that*

$$\overline{(g + X(L)) \cap G_{\text{tor}}} = \bigcup_{i \in I} \zeta + Y_i.$$

Proof of Lemma 2.3. The proof of this lemma uses (and repeats) that part of the proof of Theorem 4.3 of [11] which is correct.

Let $\sigma : L \rightarrow L$ be a field automorphism fixing K and let $P(x) \in \mathbb{Z}[x]$ be a polynomial whose complex roots do not include any roots of unity and such that $P(\sigma)$ vanishes on G_{tor} . The existence of such a pair (σ, P) is proved in [11] (cf. Corollary 3.5). Extend the difference field (L, σ) to a difference closed field (\mathbb{U}, σ) (i.e., a model of ACFA_p). Let $T := \ker P(\sigma)(\mathbb{U})$ and $F := G(\text{Fix}(\sigma))$. The main consequence of our choice of P and σ is that T and $\text{Fix}(\sigma)$ are orthogonal (cf. sections 3.2 and 3.3, and especially Lemma 3.18, of [11]).

Note the following facts:

- (i) $\Gamma^{\text{div}} \cap T = G_{\text{tor}}$
- (ii) $(\sigma - 1)(\Gamma^{\text{div}}) \subset G_{\text{tor}}$
- (iii) $P(\sigma)(\Gamma^{\text{div}}) \subset \Gamma^{\text{div}} \cap F$

Indeed, (i) and (ii) follow from the fact that σ fixes $\Gamma \leq G(K)$ pointwise and commutes with all multiplication-by- n maps. By (ii), $P(\sigma) \circ (\sigma - 1)$ vanishes on Γ^{div} . Since $P(\sigma) \circ (\sigma - 1) = (\sigma - 1) \circ P(\sigma)$, we get (iii). Now – exactly as in the proof of Theorem 4.3 of [11] – using (ii),(iii), and the fact that $P(x)$ and $x - 1$ are co-prime, one shows that $\Gamma^{\text{div}} = (\Gamma^{\text{div}} \cap T) + (\Gamma^{\text{div}} \cap F)$. By (i) this implies $\Gamma^{\text{div}} = G_{\text{tor}} + (\Gamma^{\text{div}} \cap F)$.

Let $s : G \times G \rightarrow G$ be the addition map on G , and let $\tilde{X} = s^{-1}(X)$. Now

$$\begin{aligned} X(L) \cap \Gamma^{\text{div}} &= X(\mathbb{U}) \cap \Gamma^{\text{div}} \\ &= s \left[\tilde{X}(\mathbb{U}) \cap (G_{\text{tor}} \times (\Gamma^{\text{div}} \cap F)) \right] \\ &= s \left[(\tilde{X}(\mathbb{U}) \cap (T \times F)) \cap (G_{\text{tor}} \times (\Gamma^{\text{div}} \cap F)) \right] \end{aligned}$$

The orthogonality of T and $\text{Fix}(\sigma)$ implies that there are σ -closed sets $A_1, \dots, A_\ell \subset T$ and $B_1, \dots, B_\ell \subset F$ such that

$$\tilde{X}(\mathbb{U}) \cap (T \times F) = \bigcup_{i=1}^{\ell} A_i \times B_i.$$

Letting Y_i be the Zariski closure of $G_{\text{tor}} \cap A_i$ and Z_i the Zariski closure of $\Gamma^{\text{div}} \cap B_i$, we obtain that

$$X(L) \cap \Gamma^{\text{div}} = \bigcup_{i=1}^{\ell} (Y_i(\mathbb{U}) \cap G_{\text{tor}}) + (Z_i(\mathbb{U}) \cap (\Gamma^{\text{div}} \cap F))$$

and

$$X = \bigcup_{i=1}^{\ell} Y_i + Z_i.$$

By the positive characteristic Manin-Mumford theorem (Fact 1.4) we know that each Y_i is a finite union of absolutely special subvarieties of X . Decomposing further we may assume that each Y_i is itself absolutely special.

We now show that these Y_1, \dots, Y_ℓ satisfy the conclusion of Lemma 2.3. Suppose $g \in \Gamma^{\text{div}}$, and write $g = \zeta + \eta$ where $\zeta \in G_{\text{tor}}$ and $\eta \in \Gamma^{\text{div}} \cap F$. Let $I := \{i : -\eta \in Z_i\}$. Fix $i \in I$ and suppose $y \in Y_i$. Then $y - \eta \in Y_i + Z_i \subset X$ and so $y \in (\eta + X(L))$. That is, $Y_i \subset (\eta + X(L))$, and so $Y_i \subset \overline{(\eta + X(L)) \cap G_{\text{tor}}}$. On the other hand, suppose $t \in (\eta + X(L)) \cap G_{\text{tor}}$. Then $t - \eta \in X(L)$ and so $(t, -\eta) \in \tilde{X} \cap (T \times F)$. Hence $(t, -\eta) \in A_i \times B_i$ for some $i \leq \ell$. In particular, $-\eta \in Z_i$ (so $i \in I$) and $t \in Y_i$. That is, $(\eta + X(L)) \cap G_{\text{tor}} \subset \bigcup_{i \in I} Y_i$ and so $\overline{(\eta + X(L)) \cap G_{\text{tor}}} \subset \bigcup_{i \in I} Y_i$. We have shown that

$$\overline{(\eta + X(L)) \cap G_{\text{tor}}} = \bigcup_{i \in I} Y_i.$$

So

$$\begin{aligned} \overline{(g + X(L)) \cap G_{\text{tor}}} &= \overline{(\zeta + \eta + X(L)) \cap G_{\text{tor}}} \\ &= \zeta + \overline{(\eta + X(L)) \cap G_{\text{tor}}} \\ &= \bigcup_{i \in I} \zeta + Y_i \end{aligned}$$

as desired. \square

Let Y_1, \dots, Y_ℓ be as in Lemma 2.3. Fix $i \leq \ell$ such that $\dim Y_i > 0$, and let

$$W_i := \{w \in G : w + Y_i \subset X\}.$$

So W_i is a Zariski closed subset of G and $W_i + Y_i \subset X$. If $\dim W_i = \dim X$ then $X = W_i + y$ for all $y \in Y_i$. But the facts that $\text{Stab}(X) = 0$ and $\dim Y_i > 0$ make this impossible. Hence, $\dim W_i < \dim X$. By induction, the Zariski closure \widetilde{W}_i of $W_i \cap \Gamma^{\text{div}}$ is a finite union of special subvarieties of G .

Let $Z := \bigcup \{\widetilde{W}_i + Y_i : \dim Y_i > 0\}$. By Corollary 1.5(a), Z is a finite union of special subvarieties. Hence, if $Z = X$ we are done. We may therefore assume that Z is a proper Zariski closed subset of X . We now follow Rössler's argument [10] using Z in place of the union of all positive dimensional "linear" subvarieties of X . The only substantial modification of his argument that we require in our context is that we need Claim 2.5 to prove Lemma 2.4 below.

Let $U := X \setminus Z$. Replacing K by a finitely generated extension we may assume that Z is defined over K .

Lemma 2.4. *There exists a finite set $C \subset G(K^{\text{alg}})$ such that for all $a \in U \cap \Gamma^{\text{div}}$ and $\tau \in \text{Gal}(K^{\text{alg}}/K^{\text{per}})$, $\tau(a) - a \in C$.*

Proof of Lemma 2.4. Let $a \in \Gamma^{\text{div}}$. We first point out that $G_{\text{tor}} \cap (U - a)$ is finite, and its cardinality is bounded independently of a . Indeed,

$$(G_{\text{tor}} \cap (U - a)) \cup (G_{\text{tor}} \cap (Z - a)) = G_{\text{tor}} \cap (X - a) = \bigcup_{i \in I} \zeta + Y_i$$

for some $I \subset \{1, \dots, \ell\}$ and $\zeta \in G_{\text{tor}}$ by Lemma 2.3. Fix $i \in I$ such that $\dim Y_i > 0$. As $a + \zeta + Y_i \subset X$, $a + \zeta \in W_i$. On the other hand, $a \in \Gamma^{\text{div}}$ and $\zeta \in G_{\text{tor}} \leq \Gamma^{\text{div}}$. So $a + \zeta \in \widetilde{W}_i$, which implies that $a + \zeta + Y_i \subset Z$. Hence $(\zeta + Y_i) \cap (U - a) = \emptyset$. That is, $G_{\text{tor}} \cap (U - a)$ is contained in the finite set $\{\zeta + Y_i \mid 1 \leq i \leq \ell \text{ and } \dim(Y_i) = 0\}$. The size of this latter set, say c , does not depend on a .

On the other hand, for any $a \in U \cap \Gamma^{\text{div}}$ and $\tau \in \text{Gal}(K^{\text{alg}}/K^{\text{per}})$, $\tau(a) - a \in G_{\text{tor}} \cap (U - a)$. Indeed, $\tau(U) = U$ as Z is defined over K , and if $na \in \Gamma$ then $n(\tau(a) - a) = \tau(na) - na = 0$. Hence $[K^{\text{per}}(a) : K^{\text{per}}]$ is bounded by c . It follows that for any $a \in U \cap \Gamma^{\text{div}}$ and $\tau \in \text{Gal}(K^{\text{alg}}/K^{\text{per}})$,

$$[K^{\text{per}}(\tau(a) - a) : K^{\text{per}}] \leq [K^{\text{per}}(a, \tau(a)) : K^{\text{per}}] \leq c^2.$$

The lemma will therefore follow from the following claim: □

Claim 2.5. *Given $d > 0$ there are only finitely many torsion points $\alpha \in G_{\text{tor}}$ such that $[K^{\text{per}}(\alpha) : K^{\text{per}}] < d$.*

Proof of Claim 2.5. First note that if $[K^{\text{per}}(\alpha) : K^{\text{per}}] < d$ then $[K(\alpha) : K]_{\text{sep}} < d$. So if α is separable over K then $[K(\alpha) : K] < d$. Hence, the set of prime-to- p torsion points on G that satisfy $[K^{\text{per}}(\alpha) : K^{\text{per}}] < d$ is finite (by Northcott's Theorem as in Lemma 2.5 of [10]). Since every torsion point on G is the sum of a prime-to- p torsion point and a p -primary torsion point, it suffices to show that the set

$$N := \{\alpha \in G(L) : [K^{\text{per}}(\alpha) : K^{\text{per}}] < d, p^n \alpha = 0 \text{ for some } n\}$$

is finite.

First we prove that there are only finitely many p -primary torsion points in $G(E^{\text{per}})$ for any finitely generated field $E \geq K$ (and hence in fact only finitely many torsion at all in $G(E^{\text{per}})$). Let

$$1 \rightarrow T \rightarrow G \rightarrow A \rightarrow 0$$

be an exact sequence of algebraic groups, where T is a torus and A is an abelian variety. Replacing E by a finitely generated extension, we may assume that the above exact sequence of algebraic groups is defined over E . Because the p -primary part of T_{tor} is trivial (recall that T is isomorphic to a power of the multiplicative group in characteristic p), we conclude that the p -primary part of $G(E^{\text{per}})$ injects into the p -primary part of $A(E^{\text{per}})$. Hence, it suffices to show that the p -primary

part of $A(E^{\text{per}})$ is finite. At the expense of replacing E by a finite extension, we may assume $A[p] \subset A(E)$.

As explained in Lemma 3.2 of [11], we can find a discrete valuation ring R whose fraction field is E and whose residue field is finite, such that its corresponding place v of E is of good reduction for A , and moreover, the reduction at v is injective on $A[p]$ (in the language from [11], this means that we can find a DVR R and an abelian scheme \mathfrak{A} such that its generic fibre is A , and its special fibre is an abelian variety which has the same p -rank as A). Because A is a projective variety, $A(R) = A(E)$ and so, reducing the E -points of A at v is a well-defined notion. For every $n \geq 1$, there exists a unique place of E^{1/p^n} which lies above v . By abuse of language, we may also call it v . Because the reduction at v is injective on $A[p]$, then the reduction at v is also injective on all the p -primary torsion of $A(E^{1/p^n})$, for each $n \geq 1$. However, the residue field of each extension of v on E^{1/p^n} is the same finite field for each n (because E^{1/p^n} is a purely inseparable extension of E). Thus, reduction at v embeds the p -primary torsion of $A(E^{\text{per}})$ into a finite set. We conclude that there are only finitely many p -primary torsion points in $A(E^{\text{per}})$, and so, only finitely many p -primary torsion points in $G(E^{\text{per}})$.

We continue the proof of Claim 2.5. Assume toward a contradiction that N is infinite. Note that for each $\alpha \in N$, $p\alpha \in N$. Consider the tree whose nodes are elements of N , and for a node α the set of nodes immediately above α is $\{\beta \in N : p\beta = \alpha\}$. This is an infinite but finitely branching tree – hence there must be an infinite branch. That is, there exists $(\alpha_n : n \in \omega)$ such that each $\alpha_i \in N$, $\alpha_0 = 0$, and $p\alpha_{n+1} = \alpha_n$ for all n . Using the fact that for $\alpha \in N$, $[K(\alpha) : K]_{\text{sep}} < d$, we conclude that there exists $n_0 \geq 1$ such that for every $n > n_0$, $[K(\alpha_n) : K(\alpha_{n_0})]_{\text{sep}} = 1$. This implies that $\{\alpha_n : n \in \omega\} \subset G(K(\alpha_{n_0})^{\text{per}})$. Setting $E := K(\alpha_{n_0})$, we have contradicted what we proved in the previous paragraph. Hence N must be finite. \square

We now complete the proof of Theorem 2.2.

Since Z is a proper Zariski closed subset of X , $U \cap \Gamma^{\text{div}}$ is Zariski dense in X . Hence, either $(U \cap \Gamma^{\text{div}}) \setminus G(K^{\text{per}})$ or $U \cap \Gamma^{\text{div}} \cap G(K^{\text{per}})$ is Zariski dense in X . Suppose (toward a contradiction) that the former holds. Note that for any $a \in U \cap \Gamma^{\text{div}} \setminus G(K^{\text{per}})$, there is an automorphism $\tau \in \text{Gal}(K^{\text{alg}}/K^{\text{per}})$ such that $\tau(a) - a \neq 0$ and $\tau(a) - a \in C$, where C is the finite set given by Lemma 2.4. Hence there exists $t \neq 0$ such that

$$A := \{a \in U \cap G(K^{\text{alg}}) : \tau(a) - a = t \text{ for some } \tau \in \text{Gal}(K^{\text{alg}}/K^{\text{per}})\}$$

is Zariski dense in X . But for $a \in A$, $t + a = \tau(a) \in X$. So $t \in \text{Stab}(X)$, contradicting the fact that $\text{Stab}(X) = 0$. It must therefore be the case that $U \cap \Gamma^{\text{div}} \cap G(K^{\text{per}})$ is Zariski dense in X . So

$$X(L) \cap (\Gamma^{\text{div}} \cap G(K^{\text{per}}))$$

is Zariski dense in X , and Conjecture 2.1 (our assumption) implies that X is special. This proves Theorem 2.2. \square

Remark 2.6. If we strengthen the conjectures so that the conclusions state that X is Λ -special (rather than just special), then the above proof of Theorem 2.2 shows that the strengthened Conjecture 2.1 implies the strengthened Conjecture 1.2.

Using the reduction given by Theorem 2.2, together with a result of Kim's [4], we can resolve the curve case of the full Mordell-Lang conjecture:

Corollary 2.7 (Full Mordell-Lang for Curves). *Suppose C is a smooth projective curve embedded in its jacobian A , and $\Lambda \leq A(L)$ is of finite rank. If $C \cap \Lambda$ is infinite then C is special.*

Proof. By Theorem 2.2 we need only consider the case when $\Lambda \leq A(K^{\text{per}})$ for K a finitely generated field over which A and C are defined. It suffices to show that if $C(K^{\text{per}})$ is infinite then C is special.

If the genus of C is 1 then $C = A$ is special. Hence, we may assume that the genus of C is greater than 1. Now C is birationally equivalent to an affine plane curve $C' \subset \mathbb{A}^2$ of genus greater than 1. Extending K if necessary, we may assume that the birational equivalence is over K , and hence $C'(K^{\text{per}})$ is infinite. Now Corollary 1 of [4] states that an affine plane curve of genus greater than 1 with infinitely many K^{per} -rational points must be birational to one defined over a finite field. Hence, there exists a smooth projective curve C_0 defined over $\mathbb{F}_p^{\text{alg}}$ that is birationally equivalent, and hence isomorphic, to C . It follows that there is an isomorphism $h : A \rightarrow A_0$, where A_0 is the jacobian of C_0 (also defined over $\mathbb{F}_p^{\text{alg}}$) with $h(C) = C_0$. So C is special, as desired. \square

3. THE ISOTRIVIAL CASE

Here we consider the case of semiabelian varieties defined over finite fields.

Fix L an algebraically closed field of characteristic $p > 0$ and G a semiabelian variety defined over the finite field \mathbb{F}_q , where q is a power of p . Let F denote the endomorphism of G induced by the q -power Frobenius, and denote by $\mathbb{Z}[F]$ the subring of the endomorphism ring of G generated by F .

Fact 3.1. *F is integral over \mathbb{Z} in $\text{End}(G)$. Moreover, the minimal monic polynomial of F over \mathbb{Z} has roots whose absolute values are all either q or \sqrt{q} .*

Proof. Let $r > 0$ be such that there exists a short exact sequence

$$1 \rightarrow T \rightarrow G \rightarrow A \rightarrow 0$$

defined over \mathbb{F}_{q^r} , where T is an algebraic torus and A is an abelian variety. Moreover, choose r so that T is isomorphic over \mathbb{F}_{q^r} to a power of the multiplicative group, say \mathbb{G}_m^μ for some $\mu \in \mathbb{N}$. Note that if F^r is integral over \mathbb{Z} and $P(X)$ is its minimal monic polynomial, then F is integral over \mathbb{Z} and the minimal monic polynomial of F divides $P(X^r)$. Hence it suffices to prove that F^r is integral over \mathbb{Z} and that its minimal monic polynomial has roots whose absolute values are all either q^r or $\sqrt{q^r}$. In other words we may assume that $r = 1$ and that the above exact sequence as well as the isomorphism between T and \mathbb{G}_m^μ are defined over \mathbb{F}_q .

If $G = T$ then the fact is clear since $F = q$ in $\text{End}(\mathbb{G}_m^\mu)$. For $G = A$ this is the Riemann hypothesis (see for example Theorem 14.1 of [6]). In general, use the fact that $\text{End}(G)$ embeds into $\text{End}(T) \times \text{End}(A)$ since there are no nontrivial homomorphisms from T to A or vice versa. \square

It follows that $\mathbb{Z}[F]$ is a finite integral extension of \mathbb{Z} . In particular, every finitely generated $\mathbb{Z}[F]$ -module is a finitely generated group.

3.1. F -sets and bi- F -sets. We will be interested in the intersection of subvarieties of G with certain $\mathbb{Z}[F]$ -submodules of $G(L)$. In the case of finitely generated $\mathbb{Z}[F]$ -submodules, such intersections were described in [8] in terms of the following kinds of sets:

Definition 3.2 (cf. Section 2 of [7]). Suppose $\Gamma \leq G(L)$ is a $\mathbb{Z}[F]$ -submodule.

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

$$S(a_1, \dots, a_m; \delta_1, \dots, \delta_m) := \sum_{j=1}^m \{F^{n\delta_j} a_j : n \in \mathbb{N}\}$$

where $a_1, \dots, a_m \in \Gamma$ and $\delta_1, \dots, \delta_m$ are positive integers. If all the δ_j 's are the same and equal to δ , then we simply write $S(a_1, \dots, a_m; \delta)$ for this set.

(b) By a *sum of F -cycles* in Γ we mean a set of the form

$$C(a_1, \dots, a_m; \delta_1, \dots, \delta_m) := \sum_{j=1}^m \{a_j + F^{\delta_j} a_j + F^{2\delta_j} a_j + \dots + F^{n\delta_j} a_j : n \in \mathbb{N}\}$$

where $a_1, \dots, a_m \in \Gamma$ and $\delta_1, \dots, \delta_m$ are positive integers. If all the δ_j 's are the same and equal to δ , then we simply write $C(a_1, \dots, a_m; \delta)$ for this set.

(c) An *F -set* in Γ is a set of the form $b + C + \Lambda$ where $b \in \Gamma$, C is a sum of F -cycles in Γ , and $\Lambda \leq \Gamma$ is a $\mathbb{Z}[F^r]$ -submodule for some $r > 0$.

Remark 3.3. If $\delta = r\gamma$ then $S(a; \gamma) = \bigcup_{\ell=0}^{r-1} S(F^{\ell\gamma} a; \delta)$. Hence, if δ is divisible by each of $\delta_1, \dots, \delta_n$, then $S(a_1, \dots, a_n; \delta_1, \dots, \delta_n)$ is a finite union of sets of the form $S(b_1, \dots, b_n, \delta)$.

Note that as F commutes with multiplication by any integer, if $\Gamma \leq G(L)$ is a $\mathbb{Z}[F]$ -module, then so is Γ^{div} . The following lemma says that in Γ^{div} one can ignore the F -cycles and deal only with F -orbits.

Lemma 3.4. *Every sum of F -cycles in Γ is a translate of a sum of F -orbits in Γ^{div} . In particular, every F -set in Γ^{div} is of the form $b + S + \Lambda$ where $b \in \Gamma^{\text{div}}$, S is a sum of F -orbits in Γ^{div} , and $\Lambda \leq \Gamma^{\text{div}}$ is a $\mathbb{Z}[F^r]$ -submodule for some $r > 0$.*

Proof. By Lemmas 2.7 and 7.1 of [8] every sum of F -cycles in Γ is a translate of a sum of F -orbits in some finitely generated $\mathbb{Z}[F]$ -module extension $\Gamma' \leq G(L)$ of Γ . In fact, Γ' is obtained by a finite sequence of “splitting extensions” – that is, extensions generated by elements x of $G(L)$ satisfying $F^\delta x - x - b = 0$ for some $\delta > 0$ and $b \in \Gamma$. It suffices to show therefore that such x are in Γ^{div} .

Let $P(X)$ be the minimal monic polynomial for $h := F^\delta - 1$ over \mathbb{Z} and let ℓ be the constant term of P . Note that h is an isogeny (its kernel is $G(\mathbb{F}_{q^\delta})$) and hence not a zero-divisor in $\text{End}(G)$. It follows that $\ell \neq 0$. Factoring h out of $P(h) - \ell$ we have that $-\ell = Q(h)h$ for some non-zero polynomial $Q(X)$. So $-\ell x = Q(h)(h(x))$. Since $h(x) = b \in \Gamma$, $-\ell x \in \Gamma$, and so $x \in \Gamma^{\text{div}}$ as claimed. \square

The following “absolute” isotrivial Mordell-Lang statement for finitely generated $\mathbb{Z}[F]$ -modules is why F -sets were introduced.

Fact 3.5 (Theorem 7.8 and Corollary 7.15 of [8]). *Suppose $X \subset G$ is a subvariety and $\Gamma \leq G(L)$ is a finitely generated $\mathbb{Z}[F]$ -module. Then $X(L) \cap \Gamma$ is a finite union of F -sets in Γ .*

Moreover, this happens uniformly: suppose $\{X_b\}_{b \in B}$ is an algebraic family of subvarieties of G . Then there exist F -sets A_1, \dots, A_ℓ in Γ such that for any $b \in B$ there exist $I \subset \{1, \dots, \ell\}$ and points $(g_i)_{i \in I}$ from Γ such that

$$X_b(L) \cap \Gamma = \bigcup_{i \in I} g_i + A_i.$$

One of the goals of the current paper, accomplished in Section 3.3 below, is to extend the above description to sets of the form $X(L) \cap \Gamma^{\text{div}}$. In order to do this we need to allow for negative powers of F .

Lemma 3.6. *If $\Gamma \leq G(L)$ is a $\mathbb{Z}[F]$ -submodule, then $F^{-1}(\Gamma^{\text{div}}) = \Gamma^{\text{div}}$.*

Proof. As Γ^{div} is a $\mathbb{Z}[F]$ -module, it suffices to show that for $g \in G(L)$, if $F(g) \in \Gamma^{\text{div}}$ then $g \in \Gamma^{\text{div}}$. Now the constant term of the minimal monic polynomial $P(X)$ of F over \mathbb{Z} is non-zero – it is in fact $\ell = \pm q^r$ for some $r > 0$. So for some polynomial $Q(X)$, $\ell = Q(F)F$ in $\text{End}(G)$. Hence, if $F(g) \in \Gamma^{\text{div}}$ then $Q(F)(F(g)) \in \Gamma^{\text{div}}$ and so $\ell g \in \Gamma^{\text{div}}$, and so $g \in \Gamma^{\text{div}}$ as desired. \square

Definition 3.7. Suppose $\Gamma = \Gamma^{\text{div}} \leq G(L)$ is a $\mathbb{Z}[F]$ -submodule.

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

$$B(a_1, \dots, a_m; \delta_1, \dots, \delta_m) := \sum_{j=1}^m \{F^{n\delta_j} a_j : n \in \mathbb{Z}\}$$

where $a_1, \dots, a_m \in \Gamma$ and $\delta_1, \dots, \delta_m$ are positive integers. If all the δ_j 's are the same and equal to δ , then we simply write $B(a_1, \dots, a_m; \delta)$ for this set.

(b) A *bi- F -set* in Γ is a set of the form $b + B + \Lambda$ where $b \in \Gamma$, B is a sum of bi- F -orbits in Γ , and $\Lambda \leq \Gamma$ is a $\mathbb{Z}[F^r]$ -submodule for some $r > 0$.

3.2. Full Mordell-Lang for isotrivial semiabelian varieties. Before giving an explicit description of sets of the form $X(L) \cap \Gamma^{\text{div}}$ we first prove the full function-field Mordell-Lang conjecture (Conjecture 1.2) in this case where G is defined over a finite field. The key ingredient, besides the reduction obtained in Section 2, is the explicit description of the sets $X(L) \cap \Gamma$ obtained by Scanlon and the second author in [8], and stated as Fact 3.5 above. More precisely, it is the uniformity of this description as X varies in an algebraic family that is essential.

Lemma 3.8. *Suppose $K \leq L$ is a finitely generated field. If $\Gamma \leq G(K)$ is a finitely generated group then $\Gamma^{\text{div}} \cap G(K)$ is a finitely generated group.*

Proof. After taking a finite extension of K , we may assume that, over K , G is an extension of an abelian variety A by a torus T , and that T is isomorphic to \mathbb{G}_m^μ over K . In the case that $G = A$ the lemma follows from the fact that $A(K)$ is itself finitely generated.

Consider the case when $G = T$. Let $R \leq K$ be an integrally closed finitely generated \mathbb{F}_q -algebra such that $\Gamma \leq T(R)$, T is isomorphic to \mathbb{G}_m^μ over R , and K is the fraction field of R . Then $T(R)$ is finitely generated. Moreover, by integrality, $\mathbb{G}_m^\mu(R)^{\text{div}} \cap \mathbb{G}_m^\mu(K) = \mathbb{G}_m^\mu(R)$. Hence $T(R)^{\text{div}} \cap T(K) = T(R)$, and the lemma is true in this case also.

Finally, consider the general case. Let $\pi : G \rightarrow A$ be a surjective homomorphism over K such that $T = \ker(\pi)$. Then

$$\pi(\Gamma^{\text{div}} \cap G(K)) \leq (\pi\Gamma)^{\text{div}} \cap A(K)$$

and

$$(\Gamma^{\text{div}} \cap G(K)) \cap \ker(\pi) = (T(L) \cap \Gamma)^{\text{div}} \cap T(K)$$

are both finitely generated. Hence $\Gamma^{\text{div}} \cap G(K)$, being an extension of a finitely generated group by a finitely generated group, is itself finitely generated. \square

Proposition 3.9. *Suppose $\Gamma \leq G(L)$ is a finitely generated $\mathbb{Z}[F]$ -submodule and $X \subset G$ is an irreducible subvariety. If $X(L) \cap (\bigcup_{n \geq 0} F^{-n}\Gamma)$ is Zariski dense in X then for some $n \geq 0$, $X(L) \cap F^{-n}\Gamma$ is Zariski dense in X .*

Proof. For each n , let Y_n be the Zariski closure of $X(L) \cap F^{-n}\Gamma$. We need to show that for some n , $Y_n = X$. Since the Y_n 's form a countable increasing chain of subvarieties of X whose union is Zariski-dense in X , it suffices to show that for some N , $Y_n = Y_{n+1}$ for all $n > N$. Since $\dim Y_n \leq \dim X$, it will suffice to show that the number of irreducible components of Y_n is bounded as n varies. This is what we will show.

For each n , let $X^{(n)} \subset G$ denote the transformation of X under the q^n th power Frobenius. Note that F^n is a bijection between $X(L) \cap F^{-n}\Gamma$ and $X^{(n)}(L) \cap \Gamma$. So F^n is a bijective morphism from Y_n to the Zariski closure of $X^{(n)}(L) \cap \Gamma$.

Since Γ is finitely generated, Fact 3.5 tells us that $X^{(n)}(L) \cap \Gamma$ is a finite union of F -sets. But more is true: since all the $X^{(n)}$ belong to an algebraic family of subvarieties of G , this happens uniformly. There exist F -sets A_1, \dots, A_ℓ in Γ such that for any n there exist $I \subset \{1, \dots, \ell\}$ and elements $(g_i)_{i \in I}$ from Γ , such that

$$X^{(n)}(L) \cap \Gamma = \bigcup_{i \in I} g_i + A_i.$$

Hence the number of irreducible components of the Zariski closure of $X^{(n)}(L) \cap \Gamma$ is bounded independently of n – it is bounded by the sum of the number of irreducible components of the Zariski closures of the A_i 's. Taking preimages under the bijective morphism F^n , we see that the number of irreducible components of Y_n is bounded independently of n , as desired. \square

Corollary 3.10. *Suppose $K \leq L$ is a finitely generated field and $\Lambda \leq G(K^{\text{per}})$ is a finite rank subgroup. Suppose $X \subset G$ is an irreducible subvariety such that $X(L) \cap \Lambda$ is Zariski dense in X . Then X is special.*

More precisely, some translate of X by an element of the divisible hull of the $\mathbb{Z}[F]$ -module generated by Λ is defined over a finite field.

Proof. Since Λ is a finite rank subgroup of $G(K^{\text{per}})$, there is a finitely generated subgroup of $G(K^{\text{per}})$ in whose divisible hull Λ is contained. Let Γ be the $\mathbb{Z}[F]$ -module generated by such a finitely generated group. Replacing K by a finite extension contained in K^{per} , we may assume that $\Gamma \leq G(K)$. By Lemma 3.8, $\Gamma^{\text{div}} \cap G(K)$ is finitely generated. Hence, without changing the divisible hull, we may assume $\Gamma = \Gamma^{\text{div}} \cap G(K)$.

We will show that some translate of X by an element of Γ^{div} is defined over a finite field.

Let $\widehat{\Gamma} := \Gamma^{\text{div}} \cap G(K^{\text{per}})$. So $\Lambda \subset \widehat{\Gamma}$. We claim that $\widehat{\Gamma} = \bigcup_{n \geq 0} F^{-n}\Gamma$. Indeed, it

suffices to show that $F^{-n}\Gamma = \widehat{\Gamma} \cap G(K^{\frac{1}{q^n}})$. Let $Q(X)$ be the minimal polynomial for F^n in $\mathbb{Z}[F]$ and let ℓ be the constant term of Q . Since F^n is not a zero-divisor, $\ell \neq 0$. Factoring F^n out of $Q(F^n) - \ell$ we have that $-\ell = R(F^n)F^n$ for some polynomial $R(X)$. So, for $g \in G(L)$, if $F^n g \in \Gamma$ then $-\ell g \in \Gamma$, and so $g \in \Gamma^{\text{div}}$. On the other hand, if $F^n g \in \Gamma$ then $g \in G(K^{\text{per}})$. Hence $F^{-n}\Gamma \subset \widehat{\Gamma}$. Now,

$$\widehat{\Gamma} \cap G(K^{\frac{1}{q^n}}) \subset F^{-n}\widehat{\Gamma} \cap G(K^{\frac{1}{q^n}}) = F^{-n}(\widehat{\Gamma} \cap G(K)) = F^{-n}\Gamma \subset \widehat{\Gamma} \cap G(K^{\frac{1}{q^n}}).$$

where the second equality is by the fact that $\Gamma = \Gamma^{\text{div}} \cap G(K) = \widehat{\Gamma} \cap G(K)$. Hence $F^{-n}\Gamma = \widehat{\Gamma} \cap G(K^{\frac{1}{q^n}})$. Hence $\widehat{\Gamma} = \bigcup_{n \geq 0} F^{-n}\Gamma$, as claimed.

Since $X(L) \cap \widehat{\Gamma}$ is Zariski dense in X , Proposition 3.9 implies that for some $n \geq 0$, $X(L) \cap F^{-n}\Gamma$ is Zariski dense in X . At this point, since $F^{-n}\Gamma$ is a finitely generated group, Theorem 1.1 already implies that X is special.¹ To get the more precise statement claimed we need to argue further using Lemma 3.4 as follows.

Since $\Gamma_n := F^{-n}\Gamma$ is a finitely generated $\mathbb{Z}[F]$ -module, $X(L) \cap \Gamma_n$ is a finite union of F -sets in Γ_n by Fact 3.5. By irreducibility there exist a $\mathbb{Z}[F^n]$ -submodule $H \leq \Gamma_n$ and a translate of a sum of F -cycles C in Γ_n such that $C + H$ is Zariski dense in X . By Lemma 3.4, C is a translate of a sum of F -orbits in Γ_n^{div} . But $\Gamma \leq \Gamma_n \leq \widehat{\Gamma} \leq \Gamma^{\text{div}}$ and so $\Gamma_n^{\text{div}} = \Gamma^{\text{div}}$. Hence $C = d + A$ where $d \in \Gamma^{\text{div}}$ and A is a sum of F -orbits in Γ^{div} . So $A + H$ is Zariski dense in $-d + X$. But for some $\delta > 0$, $F^\delta(A + H) \subset A + H$. It follows that $-d + X$ is defined over a finite field. \square

The following corollary is Conjecture 1.2 for isotrivial semiabelian varieties.

Theorem 3.11 (Full Isotrivial Mordell-Lang). *Let L be an algebraically closed field of characteristic $p > 0$, G a semiabelian variety defined over \mathbb{F}_q , $\Lambda \leq G(L)$ a finite rank subgroup, and $X \subset G$ an irreducible subvariety. If $X(L) \cap \Lambda$ is Zariski-dense in X , then X is special.*

Proof. By Theorem 2.2 it suffices to prove the theorem in the case that $\Lambda \leq G(K^{\text{per}})$ for some finitely generated field K . This is done in Corollary 3.10. \square

Remark 3.12. If in Theorem 3.11 we assume that Λ is in addition a $\mathbb{Z}[F]$ -submodule, then we can in fact conclude that X is Λ -special. Indeed, this is by Remark 2.6 and the ‘‘more precisely’’ clause of Corollary 3.10. For example, if $R \leq L$ is a finitely generated \mathbb{F}_q -algebra and $X(L) \cap G(R)^{\text{div}}$ is Zariski dense in X , then X is $G(R)$ -special.

3.3. Division points on subvarieties of isotrivial semiabelian varieties. We now aim to describe the sets of the form $X(L) \cap \Gamma^{\text{div}}$ where $X \subset G$ is a subvariety and $\Gamma \leq G(L)$ is a finitely generated $\mathbb{Z}[F]$ -submodule. We will do this in two

¹The isotrivial Mordell-Lang for finitely generated subgroups, which is what is being used here, is a very special case of Theorem 1.1 that was also proved in [1] using a Hilbert scheme argument and in [8] (cf. Proposition 7.7) using elementary model theory.

steps: First we will study $X(L) \cap \Gamma^S$, where Γ^S introduced below is a certain $\mathbb{Z}[F]$ -submodule of Γ^{div} that contains the prime-to- p divisible hull of Γ . Then, proving that $\Gamma^{\text{div}} = \bigcup_{n \geq 0} F^{-n}\Gamma^S$, we will give a complete description of $X(L) \cap \Gamma^{\text{div}}$.

Definition 3.13. Let $S \subset \text{End}(G)$ be the multiplicative set

$$S := \{Q(F) \in \mathbb{Z}[F] : Q(X) \in \mathbb{Z}[X] \text{ such that } Q(0) \text{ is coprime with } p\}.$$

Suppose $\Gamma \leq G(L)$ is a $\mathbb{Z}[F]$ -submodule. By the S -divisible hull of Γ we mean

$$\Gamma^S := \{g \in G(L) : \alpha(g) \in \Gamma \text{ for some } \alpha \in S\}.$$

Lemma 3.14. *Every endomorphism in S is a separable isogeny.*

Proof. Let $\alpha = Q(F) \in S$ where $Q(X) = n + XR(X) \in \mathbb{Z}[X]$ and n is coprime with p . Then $\alpha = n + FR(F)$ and hence α has the same differential as multiplication-by- n . As multiplication-by- n is a separable isogeny, so is α . \square

We collect together in the following lemma the relevant properties of the S -divisible hull and its relation to the full divisible hull:

Lemma 3.15. *Suppose $\Gamma \leq G(L)$ is a $\mathbb{Z}[F]$ -submodule.*

- (a) Γ^S is a $\mathbb{Z}[F]$ -submodule of Γ^{div} .
- (b) $\Gamma^S = \Gamma + F(\Gamma^S)$
- (c) If Γ is finitely generated as a $\mathbb{Z}[F]$ -module then $\Gamma^S/F(\Gamma^S)$ is finite.
- (d) If $\Gamma \leq G(K)$ for some subfield $K \leq L$, then $\Gamma^S \leq G(K^{\text{sep}})$.
- (e) $\Gamma^{\text{div}} = \bigcup_{n \geq 0} F^{-n}\Gamma^S$.

Proof. Using the fact that F commutes with everything in $\mathbb{Z}[F]$, it is not hard to see that Γ^S is a $\mathbb{Z}[F]$ -module. Now suppose $g \in \Gamma^S$ and so $\alpha(g) \in \Gamma$ for some $\alpha \in S$. Note that as α is an isogeny (Lemma 3.14) it cannot be a zero-divisor in $\text{End}(G)$, and hence the constant term of the minimal monic polynomial of α over \mathbb{Z} in $\text{End}(G)$ is non-zero. So there is a non-zero integer ℓ , and a polynomial $Q(X) \in \mathbb{Z}[X]$, such that $\ell = Q(\alpha)\alpha$ in $\text{End}(G)$. On the other hand, as $Q(\alpha) \in \mathbb{Z}[F]$ and Γ is a $\mathbb{Z}[F]$ -module, $Q(\alpha)(\alpha(g)) \in \Gamma$. So $\ell g \in \Gamma$, and hence $g \in \Gamma^{\text{div}}$. This proves part (a).

Let $\pm q^r$ be the constant term of the minimal monic polynomial of F over \mathbb{Z} (cf. Fact 3.1). Then $q^r \in F\mathbb{Z}[F]$, and so $\mathbb{Z}[F]/(F)$ is a quotient of $\mathbb{Z}/q^r\mathbb{Z}$. In particular, if n is coprime with p then there is an $m \in \mathbb{Z}$ such that $mn = 1$ in $\mathbb{Z}[F]/(F)$. We use this to prove that $\Gamma^S = \Gamma + F(\Gamma^S)$. Indeed, let $g \in \Gamma^S$. Then, $\alpha(g) \in \Gamma$ for some $\alpha \in S$. As the constant term of α is coprime with p , there is an integer m and some $\beta \in \mathbb{Z}[F]$ such that $m\alpha = 1 + F\beta$ in $\text{End}(G)$. Hence $m\alpha(g) = g + F\beta(g) \in g + F(\Gamma^S)$. On the other hand, $m\alpha(g) \in \Gamma$. So $g \in \Gamma + F(\Gamma^S)$, as desired for part (b).

Using part (b) we have that

$$\Gamma^S/F(\Gamma^S) = (\Gamma + F(\Gamma^S))/F(\Gamma^S) \approx \Gamma/(\Gamma \cap F(\Gamma^S))$$

and the latter is a quotient of $\Gamma/F\Gamma$. If Γ is finitely generated then $\Gamma/F\Gamma$ is a finitely generated $\mathbb{Z}[F]/(F)$ -module, and we have already seen that $\mathbb{Z}[F]/(F)$ is a quotient of the finite ring $\mathbb{Z}/q^r\mathbb{Z}$. Hence, $\Gamma^S/F(\Gamma^S)$ is finite, proving part (c).

Part (d) is a consequence of Lemma 3.14.

The right-to-left containment of part (e) follows from part (a) together with the fact (Lemma 3.6) that $F\Gamma^{\text{div}} = \Gamma^{\text{div}}$. For the left-to-right containment of part (e) we begin with the following claim.

Claim 3.16. *There exists $i \in \mathbb{N}$ such that for any $g \in G(L)$, if $pg \in \Gamma^S$ then $F^i(g) \in \Gamma^S$.*

Proof of Claim 3.16. Write the minimal monic polynomial of $F \in \mathbb{Z}[F]$ as

$$a_0 + a_1X + \cdots + a_mX^m.$$

In fact $a_0 = \pm q^r$ and $a_m = 1$. So there is a least $0 < i \leq m$ such that a_i is not divisible by p . Let $\alpha := -a_i - a_{i+1}F - \cdots - a_mF^{m-i} \in S$. Note that $a_0 + a_1F + \cdots + a_{i-1}F^{i-1} = F^i\alpha$. On the other hand, $(a_0 + a_1F + \cdots + a_{i-1}F^{i-1})(g) \in \Gamma^S$ since each a_j is divisible by p for all $j < i$ and $pg \in \Gamma^S$ by assumption. Hence $\alpha F^i(g) = F^i\alpha(g) \in \Gamma^S$, and so $F^i(g) \in \Gamma^S$ as desired. \square

Claim 3.17. *For each $n \geq 0$ there exists $k \in \mathbb{N}$ such that for any $g \in G(L)$, if $p^n g \in \Gamma^S$ then $F^k g \in \Gamma^S$.*

Proof of Claim 3.17. By induction on n . The case of $n = 0$ is clear and the case of $n = 1$ is just Claim 3.16. Now suppose $n \geq 2$ and $g \in G(L)$ is such that $p^n g \in \Gamma^S$. By Claim 3.16 applied to $p^{n-1}g$, there is an i such that $p^{n-1}F^i(g) = F^i(p^{n-1}g) \in \Gamma^S$. By the induction hypothesis, $F^\ell F^i(g) \in \Gamma^S$ for some ℓ . Hence $k = \ell + i$ works. \square

To complete the proof of part (e), and hence of Lemma 3.15, note that the prime-to- p divisible hull of Γ is contained in Γ^S , and so Γ^{div} is the p -primary divisible hull of Γ^S . So by Claim 3.17, $\Gamma^{\text{div}} \subset \bigcup_{n \geq 0} F^{-n}\Gamma^S$. So $\Gamma^{\text{div}} = \bigcup_{n \geq 0} F^{-n}\Gamma^S$ as desired. \square

The following is a first step toward understanding the intersection of $X(L)$ with the divisible hull of a finitely generated group.

Proposition 3.18. *Suppose $\Gamma = \Theta + G(\mathbb{F}_p^{\text{alg}})$ where $\Theta \leq G(L)$ is a finitely generated $\mathbb{Z}[F]$ -submodule. If $X \subset G$ is a subvariety of G over L , then $X(L) \cap \Gamma^S$ is a finite union of sets of the form $W + Y(\mathbb{F}_p^{\text{alg}})$ where W is an F -set in Γ^S and $Y \subset G$ is a subvariety defined over $\mathbb{F}_p^{\text{alg}}$.*

Remark 3.19. (a) Since $G(\mathbb{F}_p^{\text{alg}}) = G_{\text{tor}}$, $\Theta^{\text{div}} = \Gamma^{\text{div}}$.

(b) One obtains a natural example of such a Γ by considering $G(R)$ where $R \leq L$ is a finitely generated $\mathbb{F}_p^{\text{alg}}$ -algebra (cf. [7], Section 3).

Proof of Proposition 3.18. Essentially, the proof of Theorem 3.1 of [7], which in turn relies on [8], goes through in this setting. For the sake of completeness we give the argument here. We work by induction on $\dim X$. As usual, we may assume that $X(L) \cap \Gamma^S$ is Zariski dense in X , that X is irreducible, and that X has trivial stabiliser.

Let $R \leq L$ be an integrally closed finitely generated $\mathbb{F}_p^{\text{alg}}$ -algebra such that $\Gamma \leq G(R)$. Hence $\Gamma^S \leq G(R)^S$. If we show that $X(L) \cap G(R)^S$ has the desired form, then so will $X(L) \cap \Gamma^S$. Indeed, this follows from the following two facts:

- If $W \subset G(L)$ is an F -set and $Y \subset G$ is a subvariety defined over $\mathbb{F}_p^{\text{alg}}$, then

$$(W + Y(\mathbb{F}_p^{\text{alg}})) \cap \Gamma^S = (W \cap \Gamma^S) + Y(\mathbb{F}_p^{\text{alg}})$$

since $Y(\mathbb{F}_p^{\text{alg}}) \subset \Gamma \leq \Gamma^S$.

- An F -set intersected with a $\mathbb{Z}[F]$ -submodule is a finite union of F -sets (cf. Proposition 3.9(b) of [8]).

Hence, we may assume that $\Gamma = G(R)$.

Claim 3.20. *For some $g \in G(L)$, $X - g$ is defined over $\mathbb{F}_p^{\text{alg}}$.*

Proof of Claim 3.20. As $\Gamma^S \leq \Gamma^{\text{div}} = \Theta^{\text{div}}$, Θ is finitely generated, and $X(L) \cap \Gamma^S$ is Zariski dense in X , this is just an instance of the full isotrivial Mordell-Lang theorem (Theorem 3.11). \square

Let $R \leq \tilde{R} \leq L$ be an integrally closed finitely generated $\mathbb{F}_p^{\text{alg}}$ -algebra such that $g \in G(\tilde{R})$. Exactly as before, if we show that $X(L) \cap G(\tilde{R})^S$ has the desired form, then so will $X(L) \cap \Gamma^S$. Hence, we may assume that $g \in \Gamma$. Replacing X by $X - g$, and F by an appropriate power of itself, we may thus assume that X is defined over \mathbb{F}_q .

Let E be the separable closure of the fraction field of R . So $\Gamma^S \leq G(E)$ by Lemma 3.15(d). Note that since E is the separable closure of a finitely generated extension of $\mathbb{F}_p^{\text{alg}}$, $\bigcap_n E^{q^n} = \mathbb{F}_p^{\text{alg}}$.

Claim 3.21. *There exists $n > 0$ such that if $a \in \Gamma^S \setminus F(\Gamma^S)$ then $X - a$ does not have a Zariski dense intersection with $F^n \Gamma^S$.*

Proof of Claim 3.21. Suppose this were false. Let $(a_i)_{i \in \omega}$ be a sequence of points in $\Gamma^S \setminus F(\Gamma^S)$ and $(n_i)_{i \in \omega}$ be a strictly increasing sequence of positive integers such that $X - a_i$ has a Zariski dense intersection with $F^{n_i} \Gamma^S$, and so with $G(E^{q^{n_i}})$.

Note that Γ^S is F -pure in $G(E)$. Indeed, if $g \in G(E)$ and $F(g) \in \Gamma^S$, then $\alpha F(g) \in \Gamma = G(R)$ for some $\alpha \in S$. So $F(\alpha(g)) \in G(R)$. Hence $\alpha(g) \in G(E) \cap G(R^{\frac{1}{q}})$. But $E \cap R^{\frac{1}{q}} = R$ since R is integrally closed and E is separable over the fraction field of R . Hence $g \in G(R)^S = \Gamma^S$.

It follows that $\Gamma^S \setminus F(\Gamma^S) \subset G(E) \setminus G(E^q)$. So each $a_i \in G(E) \setminus G(E^q)$. Passing to a saturated elementary extension *E we find ${}^*a \in G({}^*E) \setminus G({}^*E^q)$ such that $X - {}^*a$ has a Zariski dense intersection with $\bigcap_i G({}^*E^{q^{n_i}})$, and hence is defined over

the algebraically closed field $\bigcap_i {}^*E^{q^{n_i}}$. But since X is defined over \mathbb{F}_q we obtain

that $\sigma({}^*a) - {}^*a$ stabilises X for all automorphisms of ${}^*E^{\text{alg}}$ that fix $\bigcap_i {}^*E^{q^{n_i}}$. As

X has trivial stabiliser, ${}^*a \in G(\bigcap_i {}^*E^{q^{n_i}})$. But this contradicts ${}^*a \notin G({}^*E^q)$. \square

The rest of the argument is exactly as in [7].

By Claim 3.21, for each $a \in \Gamma^S \setminus F\Gamma^S$, $\overline{(X - a)(L) \cap F^n \Gamma^S}$ has lower dimension than X . Note that as $G(\mathbb{F}_p^{\text{alg}})$ is S -divisible, $\Gamma^S = \Theta^S + G(\mathbb{F}_p^{\text{alg}})$. Hence by Lemma 3.15(c) applied to the finitely generated Θ , $F\Gamma^S$ has finite index in Γ^S . It follows that $F^n \Gamma^S$ has finite index in $F\Gamma^S$. So $\overline{(X - a)(L) \cap F\Gamma^S}$ has lower dimension than X . Let $A \subset \Gamma^S$ be a finite set of coset representatives for the *non-zero* cosets of $F\Gamma^S$ in Γ^S . Let $Z_a := \overline{(X - a)(L) \cap F\Gamma^S}$ as above. By induction we have

that

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

where each S_i is an F -set and Y_i is a subvariety defined over $\mathbb{F}_p^{\text{alg}}$. Let m be sufficiently divisible so that each Y_i is defined over the extension of \mathbb{F}_q of degree m . Noting that since $G(\mathbb{F}_p^{\text{alg}}) \leq \Gamma^S \leq G(E)$, $F^\infty \Gamma^S = G(\mathbb{F}_p^{\text{alg}})$, we compute:

$$\begin{aligned}
 X(L) \cap \Gamma^S &= [X(L) \cap F^\infty \Gamma^S] \cup [X(L) \cap (\Gamma^S \setminus F^\infty \Gamma^S)] \\
 &= X(\mathbb{F}_p^{\text{alg}}) \cup \bigcup_{t=0}^{\infty} X(L) \cap (F^t \Gamma^S \setminus F^{t+1} \Gamma^S) \\
 &= X(\mathbb{F}_p^{\text{alg}}) \cup \bigcup_{j=0}^{\infty} \bigcup_{\ell=0}^{m-1} X(L) \cap [F^{mj+\ell} \Gamma^S \setminus F^{mj+\ell+1} \Gamma^S] \\
 &= X(\mathbb{F}_p^{\text{alg}}) \cup \bigcup_{j=0}^{\infty} F^{mj} \left[\bigcup_{\ell=0}^{m-1} F^\ell (X(L) \cap (\Gamma^S \setminus F\Gamma^S)) \right] \\
 &= X(\mathbb{F}_p^{\text{alg}}) \cup \bigcup_{j=0}^{\infty} F^{mj} \left[\bigcup_{\ell=0}^{m-1} \bigcup_{i=1}^k F^\ell S_i + Y_i^{(q^\ell)}(\mathbb{F}_p^{\text{alg}}) \right] \\
 &= X(\mathbb{F}_p^{\text{alg}}) \cup \bigcup_{\ell=0}^{m-1} \bigcup_{i=1}^k \left[\left(\bigcup_{j=0}^{\infty} F^{mj} (F^\ell S_i) \right) + Y_i^{(q^\ell)}(\mathbb{F}_p^{\text{alg}}) \right]
 \end{aligned}$$

By Corollary 7.3 of [8], fixing i and ℓ , the set $\bigcup_{j=0}^{\infty} F^{mj} (F^\ell S_i)$ is contained in some

$\bigcup_{k=1}^t T_k^{(i,\ell)}$ where $T_k^{(i,\ell)}$ are F -sets in Γ^S and $\overline{\bigcup_{j=0}^{\infty} F^{mj} (F^\ell S_i)} = \overline{\bigcup_{k=1}^t T_k^{(i,\ell)}}$. So for

any $y \in Y_i^{(q^\ell)}(\mathbb{F}_p^{\text{alg}})$, $\bigcup_{j=0}^{\infty} F^{mj} (F^\ell S_i) \subset \bigcup_{k=1}^t T_k^{(i,\ell)} \subset X - y$. Hence we may replace

$\bigcup_{j=0}^{\infty} F^{mj} (F^\ell S_i)$ with $\bigcup_{k=1}^t T_k^{(i,\ell)}$ in the above expression. That is,

$$X(L) \cap \Gamma^S = X(\mathbb{F}_p^{\text{alg}}) \cup \bigcup_{\ell=0}^{m-1} \bigcup_{i=1}^k \left[\left(\bigcup_{k=1}^t T_k^{(i,\ell)} \right) + Y_i^{(q^\ell)}(\mathbb{F}_p^{\text{alg}}) \right]$$

and hence is a set of the desired form. This proves Proposition 3.18 \square

The following lemmas extend 7.2 and 7.3 of [8] to the bi- F -set context (cf. Section 3.1 for the notation).

Lemma 3.22. *Suppose $Y \subset G$ is a subvariety defined over \mathbb{F}_{q^r} , $\Lambda \leq G(L)$ is a $\mathbb{Z}[F^r]$ -submodule, and $a_1, \dots, a_n \in G(L)$. Then,*

$$\overline{B(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})} = \overline{S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})}.$$

Moreover, this subvariety is defined over \mathbb{F}_{q^r} .

Proof. The right-to-left containment is clear. For the other direction, let $Z := \overline{S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})}$. Since

$$F^r(S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})) \subset S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}}),$$

Z is defined over \mathbb{F}_{q^r} . Now let $a \in B(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})$. Then for some $N > 0$, $F^{Nr}(a) \in S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}}) \subset Z$. Since Z is defined over \mathbb{F}_{q^r} , it follows that $a \in Z$. So $\overline{B(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})} \subset Z$, as desired. \square

Lemma 3.23. *Suppose $Y \subset G$ is a subvariety defined over \mathbb{F}_{q^r} , $\Lambda \leq G(L)$ is an F^r -divisible $\mathbb{Z}[F^r]$ -submodule, and $b, a_1, \dots, a_n \in G(L)$. If $X \subset G$ is a subvariety such that*

$$\Sigma := \bigcup_{m \geq 0} F^{-mr}(b + S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})) \subset X$$

then $\Sigma \subset \overline{B(b, a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})} \subset X$.

Proof. Since Λ is F^r -divisible and Y is defined over \mathbb{F}_{q^r} , it is not hard to verify the first containment. For the second containment we note that for all $m \geq 0$,

$$\begin{aligned} F^{-mr}b + B(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}}) &\subset F^{-mr}b + \overline{B(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})} \\ &= F^{-mr}b + \overline{S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})} \\ &= F^{-mr}(b + \overline{S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})}) \\ &\subset \overline{\Sigma} \\ &\subset X \end{aligned}$$

where the first equality is by Lemma 3.22 and the second equality is by the fact that $\overline{S(a_1, \dots, a_n; r) + \Lambda + Y(\mathbb{F}_p^{\text{alg}})}$ is defined over \mathbb{F}_{q^r} (also Lemma 3.22). \square

We are now ready to prove the following “absolute” full isotrivial Mordell-Lang statement:

Theorem 3.24. *Let L be an algebraically closed field of characteristic p , q a power of p , G a semiabelian variety defined over \mathbb{F}_q , and F the q -power Frobenius endomorphism of G . If $\Gamma \leq G(L)$ is a finitely generated $\mathbb{Z}[F]$ -submodule and $X \subset G$ is a subvariety, then $X(L) \cap \Gamma^{\text{div}}$ is a finite union of sets of the form $T + Y(\mathbb{F}_p^{\text{alg}})$ where T is a bi- F -set in Γ^{div} and $Y \subset G$ is a subvariety defined over $\mathbb{F}_p^{\text{alg}}$.*

Proof. We may assume that X is irreducible and $X \cap \Gamma^{\text{div}}$ is Zariski dense in X . Hence, by Theorem 3.11, X is special. That is, $X = d + Z$ where Z is defined over $\mathbb{F}_p^{\text{alg}}$. Moreover, by Remark 3.12, we can find $d \in \Gamma^{\text{div}}$. By Lemma 3.15(e), $\Gamma^{\text{div}} = \bigcup_{n \geq 0} F^{-n}\Gamma^S$. Say $d \in F^{-m}\Gamma^S$ and let $\Gamma_1 := F^{-m}\Gamma$. Note that $d \in \Gamma_1^S$.

Set $\Psi := \Gamma_1 + G(\mathbb{F}_p^{\text{alg}})$. As we have pointed out before, the S -divisibility of $G(\mathbb{F}_p^{\text{alg}})$ implies that $\Psi^S = \Gamma_1^S + G(\mathbb{F}_p^{\text{alg}})$. We have

$$\begin{aligned} \Gamma^{\text{div}} &= \Gamma_1^{\text{div}} \\ &= \Gamma_1^{\text{div}} + G(\mathbb{F}_p^{\text{alg}}) \\ &= \bigcup_{n \geq 0} F^{-n} \Gamma_1^S + G(\mathbb{F}_p^{\text{alg}}) \\ &= \bigcup_{n \geq 0} F^{-n} (\Gamma_1^S + G(\mathbb{F}_p^{\text{alg}})) \\ &= \bigcup_{n \geq 0} F^{-n} \Psi^S \end{aligned}$$

where the first equality is by Lemma 3.6, the third is by Lemma 3.15(e) applied to Γ_1 , and the fourth uses the fact that $F^{-n}G(\mathbb{F}_p^{\text{alg}}) = G(\mathbb{F}_p^{\text{alg}})$.

On the other hand, since Γ_1 is finitely generated, Proposition 3.18 tells us that $Z \cap \Psi^S$ is a finite union of sets of the form $W + Y(\mathbb{F}_p^{\text{alg}})$ where W is an F -set in Ψ^S and $Y \subset G$ is a subvariety defined over $\mathbb{F}_p^{\text{alg}}$. Using Lemma 3.4 we can express the W 's as F -sets in Γ^{div} that involve sums of F -orbits rather than F -cycles. Moreover, using Remark 3.3, we can choose r sufficiently divisible such that

$$Z \cap \Psi^S = \bigcup_{i=1}^{\ell} (b_i + S(a_{i,1}, \dots, a_{i,t}; r) + \Lambda_i + Y_i(\mathbb{F}_p^{\text{alg}}))$$

where $b_i, a_{i,1}, \dots, a_{i,t} \in \Gamma^{\text{div}}$, $\Lambda_i \leq \Psi^S$ is a $\mathbb{Z}[F^r]$ -module, and Z and Y_i are all defined over \mathbb{F}_{q^r} . Now

$$\begin{aligned} X \cap \Gamma^{\text{div}} &= (d + Z) \cap \left(\bigcup_{n \geq 0} F^{-n} \Psi^S \right) \\ &= d + [Z \cap \left(\bigcup_{n \geq 0} F^{-n} \Psi^S \right)] \\ &= d + [Z \cap \left(\bigcup_{n \geq 0} F^{-nr} \Psi^S \right)] \\ &= d + \bigcup_{n \geq 0} F^{-nr} (Z \cap \Psi^S) \\ &= d + \bigcup_{i=1}^{\ell} \bigcup_{n \geq 0} F^{-nr} (b_i + S(a_{i,1}, \dots, a_{i,t}; r) + \Lambda_i + Y_i(\mathbb{F}_p^{\text{alg}})) \end{aligned}$$

Since $\overline{\Lambda}_i$ and Γ^{div} are preserved under F^{-r} , replacing each Λ_i by $\overline{\Lambda}_i \cap \Gamma^{\text{div}}$ allows us to assume that each Λ_i is F^r -divisible. Hence, letting

$$\Sigma_i := \bigcup_{n \geq 0} F^{-nr} (b_i + S(a_{i,1}, \dots, a_{i,t}; r) + \Lambda_i + Y_i(\mathbb{F}_p^{\text{alg}})),$$

Lemma 3.23 gives us that

$$\Sigma_i \subset B(b_i, a_{i,1}, \dots, a_{i,t}; r) + \Lambda_i + Y_i(\mathbb{F}_p^{\text{alg}}) \subset -d + X$$

for all $i = 1, \dots, \ell$. Hence

$$X \cap \Gamma^{\text{div}} = d + \bigcup_{i=1}^{\ell} (B(b_i, a_{i,1}, \dots, a_{i,t}; r) + \Lambda_i + Y_i(\mathbb{F}_p^{\text{alg}}))$$

which is of the desired form. \square

REFERENCES

- [1] D. Abramovich and J. Voloch, *Toward a proof of the Mordell-Lang conjecture in characteristic p* , International Mathematics Research Notices (1992), no. 5, 103–115.
- [2] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, *Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics*, Proceedings of the London Mathematical Society **85** (2002), no. 3, 257–311.
- [3] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, Journal of the American Mathematical Society **9** (1996), no. 3, 667–690.
- [4] M. Kim, *Purely inseparable points on curves of higher genus*, Mathematical Research Letters **4** (1997), no. 5, 663–666.
- [5] M. McQuillan, *Division points on semi-abelian varieties*, Inventiones Mathematicae **120** (1995), no. 1, 143–159.
- [6] J.S. Milne, *Abelian varieties*, Course notes available at <http://www.jmilne.org/math/CourseNotes/math731.pdf>.
- [7] R. Moosa and T. Scanlon, *The Mordell-Lang conjecture in positive characteristic revisited*, Model theory and applications, Quaderni di matematica, vol. 11, Dipartimento di Matematica Seconda Università di Napoli, 2002, pp. 273–296.
- [8] ———, *F -structures and integral points on semiabelian varieties over finite fields*, American Journal of Mathematics **126** (2004), 473–522.
- [9] R. Pink and D. Rössler, *On ψ -invariant subvarieties of semiabelian varieties and the Manin-Mumford conjecture*, Journal of Algebraic Geometry **13** (2004), no. 4, 771–798.
- [10] D. Rössler, *An afterthought on the generalized Mordell-Lang conjecture*, To appear in the proceedings of the workshop on model theory, algebraic and analytic geometry (Newton Institute, Cambridge, July 11–15, 2005).
- [11] T. Scanlon, *Positive characteristic Manin-Mumford theorem*, Compositio Mathematica **141** (2005), no. 6, 1351–1364.

DEPARTMENT OF MATHEMATICS AND STATISTICS, MCMMASTER UNIVERSITY, 1280 MAIN STREET WEST, HAMILTON, ONTARIO, CANADA L8S 4K1
E-mail address: `dghioca@math.mcmaster.ca`

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, 200 UNIVERSITY AVENUE WEST, WATERLOO, ONTARIO, CANADA N2L 3G1
E-mail address: `rmoosa@math.uwaterloo.ca`