MULTIPLES OF SUBVARIETIES IN ALGEBRAIC GROUPS OVER FINITE FIELDS

BJORN POONEN

ABSTRACT. Let X be a subvariety of a commutative algebraic group G over $\overline{\mathbb{F}}_q$ such that X generates G. Then $\bigcup_{\phi\in\operatorname{End} G}\phi(X(\overline{\mathbb{F}}_q)) = G(\overline{\mathbb{F}}_q)$. If G is semiabelian, this can be strengthened to $\bigcup_{n\geq 1} nX(\overline{\mathbb{F}}_q) = G(\overline{\mathbb{F}}_q)$, and there is a density-1 set of primes S such that $X(\overline{\mathbb{F}}_q)$ projects surjectively onto the S-primary part of $G(\overline{\mathbb{F}}_q)$. These results build on work of Bogomolov and Tschinkel.

1. Statements of results

This introductory section states our main results; the proofs are contained in later sections. Throughout this paper, $\mathbb{F}_q$ is a finite field of q elements, and $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$.

1.1. **A result of Bogomolov and Tschinkel.** Bogomolov and Tschinkel proved the following result and used it to deduce the existence of non-uniruled K3 surfaces over $\overline{\mathbb{F}}_q$ whose rational curves cover all $\overline{\mathbb{F}}_q$-points.

Theorem 1.1 ([BT03])**.** *Let X be a smooth projective integral curve of genus $g \geq 1$ over $\overline{\mathbb{F}}_q$, embedded in its Jacobian J in the usual way, using a basepoint O. Then $J(\overline{\mathbb{F}}_q) = \bigcup_{\phi\in\operatorname{End} J}\phi(X(\overline{\mathbb{F}}_q))$.*

The first goal of this paper is to give a new proof requiring nothing deeper than the Weil conjectures for curves and the geometric class field theory fact that if $X \hookrightarrow J$ is a curve embedded in its Jacobian in the usual way and $\phi\colon A \to J$ is a separable isogeny, then $\phi^{-1}(X)$ is geometrically irreducible.

1.2. **Generalizations.** Actually this new proof works also for generalized Jacobians, so we prove the result in this generality, in Section 2.

In later sections, we generalize further to the case of a subvariety X of arbitrary dimension in an arbitrary commutative algebraic group G, subject to the obviously necessary condition that X generate G. (In this paper, an *algebraic group* over a field k is a connected reduced group scheme of finite type over k. See Section 3 for the definition of "generate".)

Theorem 1.2. *Let G be a commutative algebraic group over $\overline{\mathbb{F}}_q$. Let $X \subseteq G$ be an irreducible (but not necessarily closed) subvariety that generates G. Then $\bigcup_{\phi\in\operatorname{End} G}\phi(X(\overline{\mathbb{F}}_q)) = G(\overline{\mathbb{F}}_q)$.*

Date: November 30, 2004.

2000 *Mathematics Subject Classification.* Primary 14G15; Secondary 14K15.

Key words and phrases. Algebraic group, abelian variety, semiabelian variety, generalized Jacobian, finite field.

This research was supported by NSF grant DMS-0301280 and a Packard Fellowship. This article has been published in *Internat. Math. Res. Notices* **2005**, no. 24, 1487–1498.

Moreover, it suffices to take the union over $\phi \in \mathbb{Z}[F]$, where F is a Frobenius endomorphism of G.

Theorem 1.2 shows that each point of G is contained in the image of X under some endomorphism. In fact, given any finite collection of points of G, we can find a single endomorphism that works for all of them:

Corollary 1.3. *Under the hypotheses of Theorem 1.2, if $S \subseteq G(\overline{\mathbb{F}}_q)$ is finite, then $S \subseteq \phi(X(\overline{\mathbb{F}}_q))$ for some $\phi \in \mathbb{Z}[F] \subseteq \operatorname{End} G$.*

Proof. Apply Theorem 1.2 to $X^s \subseteq G^s$ where $s = \#S$. □

1.3. **Semiabelian varieties.** In the case where G is a semiabelian variety, we show below that instead of using all $\phi \in \operatorname{End} G$, it is enough to use the multiplication-by-n maps for $n \in \mathbb{Z}_{\geq 1}$.

Theorem 1.4. *Let G be a semiabelian variety over $\overline{\mathbb{F}}_q$. Let $X \subseteq G$ be an irreducible subvariety that generates G. Then $\bigcup_{n\geq 1} nX(\overline{\mathbb{F}}_q) = G(\overline{\mathbb{F}}_q)$.*

The crucial case where X is a curve was obtained independently by Bogomolov and Tschinkel [BT05]. (After discovering our proof, we learned that they had found their proof a few weeks earlier.)

We get a corollary analogous to Corollary 1.3, proved in the same way:

Corollary 1.5. *Under the hypotheses of Theorem 1.4, if $S \subseteq G(\overline{\mathbb{F}}_q)$ is finite, then $S \subseteq n(X(\overline{\mathbb{F}}_q))$ for some $n \geq 1$.*

Remark 1.6. The semiabelian restriction in Theorem 1.4 is necessary, as the following example shows. Let $G = \mathbb{G}_a \times \mathbb{G}_a$ with coordinates x, y, and let p be the characteristic. Let X be the curve $xy = 1$ in G. By criterion (i) of Corollary 3.3, X generates G. But $\bigcup_{n\geq 1} nX(\overline{\mathbb{F}}_q) = \bigcup_{n=1}^{p} nX(\overline{\mathbb{F}}_q)$, which is an algebraic subset of G of dimension 1. Thus $\bigcup_{n\geq 1} nX(\overline{\mathbb{F}}_q) \neq G(\overline{\mathbb{F}}_q)$.

Remark 1.7. One faces similar counterexamples if one tries to generalize Theorem 1.4 to noncommutative groups, such as semisimple algebraic groups. (One interprets n as the n-th power map in the group.) For instance, for $G = \mathrm{SL}_2$ over $\overline{\mathbb{F}}_q$ of characteristic p, if $a = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ with $\alpha \in \overline{\mathbb{F}}_q$, then a calculation shows that the only elements of $\mathrm{SL}_2(\overline{\mathbb{F}}_q)$ having a power equal to a are those of the form $\pm \begin{pmatrix} 1 & m\alpha \\ 0 & 1 \end{pmatrix}$ with $m \in \mathbb{F}_p$. If X is an irreducible curve containing one such element for every $\alpha \in \overline{\mathbb{F}}_q$, then X has infinite intersection with either $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \overline{\mathbb{F}}_q \right\}$ or $\left\{ -\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \overline{\mathbb{F}}_q \right\}$, so X is a dense open subset of one of these curves. Thus there is no curve X in SL_2 satisfying $\bigcup_{n\geq 1} nX(\overline{\mathbb{F}}_q) = \mathrm{SL}_2(\overline{\mathbb{F}}_q)$, even though one can easily construct curves that generate SL_2 as a group.

1.4. **Projections of subvarieties.** If ℓ is a prime and A is a torsion abelian group, let $A\{\ell\} = \bigcup_{e\geq 1} A[\ell^e]$ be the ℓ-primary part of A. If S is a set of primes, let $A\{S\} = \bigoplus_{\ell \in S} A\{\ell\} \subseteq A$. By the density of S, we mean natural density: see Section 6 for the definition.

The paper [BT05] proves, under the assumptions of Theorem 1.4 (for X a curve), that there exists a set S of positive density such that the restriction of the canonical projection $G(\overline{\mathbb{F}}_q) \twoheadrightarrow G(\overline{\mathbb{F}}_q)\{S\}$ to $X(\overline{\mathbb{F}}_q)$ is surjective. In fact they can find S containing any given finite set of primes. Their work extends earlier results for a curve in its Jacobian in [AI85] (where it is assumed that $\#S = 1$) and [PS03, §2] (where it is observed that the method of [AI85] works also for finite S). The paper [PS03] also considers (for finite S) the case of an arbitrary positive-dimensional subvariety X in a simple abelian variety A, by reducing to the case of curves: because their A is simple, they can sidestep the issue we must face, of whether a curve in A generates A.

Building on the ideas in [BT05], but with more work, we strengthen the result by constructing an S of density 1 for which the conclusion still holds:

Theorem 1.8. *Let G be a semiabelian variety over $\overline{\mathbb{F}}_q$. Let $X \subseteq G$ be an irreducible subvariety that generates G. Let S_0 be any finite set of primes. Then there exists a set of primes $S \supseteq S_0$ of density 1 such that the composition $X(\overline{\mathbb{F}}_q) \to G(\overline{\mathbb{F}}_q) \twoheadrightarrow G(\overline{\mathbb{F}}_q)\{S\}$ is surjective.*

This will be proved in Section 6.

2. Images of a curve under endomorphisms of a generalized Jacobian

The following statement generalizes Theorem 1.1 but we call it a lemma, because it will be used to prove the more general Theorem 1.2.

Lemma 2.1. *Let X' be a smooth projective integral curve over $\overline{\mathbb{F}}_q$. Let $\mathfrak{m}$ be a modulus, and let J be the generalized Jacobian of X' with respect to $\mathfrak{m}$, as defined in* [Ser88, Chapter I]. *Let X be the image of the map $\iota\colon X' - \mathfrak{m} \to J$ sending x to the class of $x - D$, where D is a fixed divisor of degree 1 supported on $X' - \mathfrak{m}$. Then $\bigcup_{\phi \in \operatorname{End} J} \phi(X(\overline{\mathbb{F}}_q)) = J(\overline{\mathbb{F}}_q)$.*

Proof of Theorem 1.1. We may assume $\dim J > 0$; then ι is an embedding. Suppose $a \in J(\overline{\mathbb{F}}_q)$; we must find $\phi \in \operatorname{End} J$ and $x \in X(\overline{\mathbb{F}}_q)$ such that $\phi(x) = a$. Without loss of generality, X, J, ι, and a are defined over $\mathbb{F}_q$. Let F be the q-power Frobenius endomorphism of J. We will seek $x \in X(\mathbb{F}_{q^n})$ for some large n; in this case $f_n := F^n - 1$ would kill x, while $F - 1$ kills a, so we try $\phi := 1 + F + \cdots + F^{n-1}$, which is an isogeny since its derivative is nonzero. In particular, we can choose $b \in \phi^{-1}(a)$. Then $(F^n - 1)b = (F - 1)a = 0$, so $b \in J(\mathbb{F}_{q^n})$. We hope $X(\mathbb{F}_{q^n})$ meets $\phi^{-1}(a) = b + \ker \phi = b + (F - 1)J(\mathbb{F}_{q^n})$. Equivalently, if we define $g\colon J \to J$ (over $\mathbb{F}_{q^n}$) by $g(z) = b + (F - 1)z$, we hope that $Y_n := g^{-1}(X)$ has an $\mathbb{F}_{q^n}$-point.

Over $\overline{\mathbb{F}}_q$, the curve Y_n is isomorphic to the inverse image of X under the separable isogeny $F - 1\colon J \to J$, so Y_n is geometrically irreducible by Proposition 10 in [Ser88, VI.§2.11]. Since its $\overline{\mathbb{F}}_q$-isomorphism type is independent of n and b, the Weil conjectures prove $Y_n(\mathbb{F}_{q^n}) \neq \emptyset$ if n is large enough. □

3. The subgroup generated by a subvariety

Lemma 3.1. *Let G be a nontrivial algebraic group over an algebraically closed field k. Then $G(k)$ is not cyclic.*

Proof. If $G(k)$ is cyclic, then G is commutative. By the structure theory of algebraic groups, G contains an algebraic subgroup H isomorphic to $\mathbb{G}_a$, $\mathbb{G}_m$, or a nontrivial abelian variety.

In each case, $H(k)$ has infinitely many elements of finite order, so $H(k)$ is not cyclic. Thus $G(k)$ is not cyclic. □

Lemma 3.2. *Let G be a commutative algebraic group over an algebraically closed field k. Let X be an irreducible subvariety of G, not necessarily closed. Let X_n be the image of X^n under the addition morphism $G^n \to G$. Then there exists an algebraic subgroup $H \subseteq G$ and a point $g \in G(k)$ such that $X_n \subseteq ng + H$ for all $n \geq 1$ with equality for $n \gg 1$. Moreover, H is uniquely determined by $X \subseteq G$.*

Proof. Translate X to reduce to the case $0 \in X$. Then $X_n \subseteq X_{n+1}$ for all n. Let H_n be the Zariski closure of X_n in G. Then H_n is the closure of the image of the irreducible variety X^n, so H_n is irreducible. Since $\dim G < \infty$, the sequence $H_1 \subseteq H_2 \subseteq \cdots$ is eventually constant; say $H_n = H_{n+1} = \cdots$. Define $H = H_n$. Then $H \subseteq H + H = H_n + H_n \subseteq H_{2n} = H$, so $H + H = H$. If $h \in H(k)$, then $h + H \subseteq H$, but $h + H$ and H are closed subvarieties of G of the same dimension, so $h + H = H$. In particular, $0 \in h + H$, so $-h \in H$. Thus H is an algebraic subgroup of G.

Let $m \geq 2n$. Then given $h \in H(k)$, the subvarieties X_{m-n} and $h - X_n$ are dense in $H = h - H$ so they intersect. Hence $h \in X_{m-n} + X_n = X_m$. Thus $X_m = H$ for any $m \geq 2n$. So the first conclusion holds, with $g = 0$.

Any H satisfying the first conclusion equals the image of $X_n \times X_n$ under the subtraction map $G \times G \to G$ for $n \gg 1$, so it is determined. □

Corollary 3.3. *Let notation be as in Lemma 3.2. Then the following are equivalent:*

(i) *The subvariety X is not contained in any translate of an algebraic subgroup $H \subsetneq G$.*
(ii) *There exists $n \geq 1$ such that the addition map $X^n \to G$ is surjective.*
(iii) *The set $X(k)$ generates $G(k)$ as an abstract group.*

Proof.
(i) $\implies$ (ii): Assuming (i), the H of Lemma 3.2 must be G.
(ii) $\implies$ (iii): Trivial.
(iii) $\implies$ (i): Suppose $X(k)$ generates $G(k)$. If X were contained in the translate of $H \subsetneq G$ by g, then $(G/H)(k)$ would be generated by the image of g, contradicting Lemma 3.1. □

Definition 3.4. If the equivalent conditions of Corollary 3.3 hold, we say that X *generates* G. If X and G are defined over a field that is not necessarily algebraically closed, we say that X *generates* G if it is so after extending the base field to an algebraic closure.

4. Generating curves inside generating subvarieties

This section contains the work needed to reduce the case of X of arbitrary dimension to the case of curves.

Lemma 4.1. *Let X be a geometrically irreducible quasi-projective variety over a finite field $\mathbb{F}_q$. Assume $\dim X \geq 1$. There exists a finite extension $k \supseteq \mathbb{F}_q$ such that for every finite subset $S \subseteq X(\overline{k})$ there exists a geometrically irreducible curve $Z \subseteq X_k$ containing S.*

Proof. Without loss of generality, replace X by a projective closure. Replacing $\mathbb{F}_q$ by a finite extension and X by its associated reduced subscheme, we may assume X is geometrically integral. By [dJ96, Theorem 4.1], after passing to a finite extension k, there exists a smooth projective geometrically integral $X' \subseteq \mathbb{P}^n$ and a generically finite proper morphism $\pi\colon X' \to$

X. Lift each $s \in S$ to get a finite subset $S' \in X'(\overline{k})$. By [Poo04, Corollary 3.4], there exists a geometrically irreducible curve $Z' \subseteq X'$ passing through all points of S'. Let $Z = \pi(Z')$. □

Remark 4.2. Lemma 4.1 holds also if $\mathbb{F}_q$ is replaced by an arbitrary field, because the analogue of [Poo04, Corollary 3.4] is true (and easier to prove) over infinite fields.

Lemma 4.3. *Let G be an d-dimensional commutative algebraic group over $\mathbb{F}_q$. Then*

$$(\sqrt{q}-1)^{2d} \leq \#G(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2d}.$$

Proof. Using exact sequences and Lang's theorem on the vanishing of $H^1(\mathbb{F}_q, A)$ for any algebraic group A, we reduce to the cases where G is an abelian variety, a torus, or $\mathbb{G}_a$. If G is an abelian variety, the Weil conjectures give the bounds. If G is a torus, $\#G(\mathbb{F}_q) = \det(q - F|_{\hat{G}})$ where $\hat{G}$ is the character group of G, and F is the q-power Frobenius acting on it; since some power of F acts trivially on $\hat{G}$, the eigenvalues of F are roots of unity, and the bound follows. If $G = \mathbb{G}_a$, $\#G(\mathbb{F}_q) = q$. □

Lemma 4.4. *Let G be a commutative algebraic group over $\overline{\mathbb{F}}_q$. Let $X \subseteq G$ be an irreducible subvariety. Suppose that $\dim X \geq 1$, and X generates G. Then there is an irreducible curve $Z \subseteq X$ that generates G.*

Proof. Without loss of generality, X and G are over $\mathbb{F}_q$. Replace $\mathbb{F}_q$ by the k of Lemma 4.1 for X. Enlarge $\mathbb{F}_q$ again if necessary so that $(\sqrt{q}-1)^{2d} > (\sqrt{q}+1)^{2d-2}$, where $d = \dim G$. For some $n \geq 1$, we may express each point in $G(\mathbb{F}_q)$ as $x_1 + \cdots + x_n$ with $x_i \in X(\overline{\mathbb{F}}_q)$. Lemma 4.1 gives an irreducible curve $Z \subseteq X$ passing through the points of X occurring in all these expressions. Let H be as in Lemma 3.2 for $Z \subseteq G$. By choice of Z, $H(\mathbb{F}_q) = G(\mathbb{F}_q)$. If $H \neq G$, Lemma 4.3 applied to G and H gives

$$(\sqrt{q}-1)^{2d} \leq \#G(\mathbb{F}_q) = \#H(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2d-2},$$

contradicting our earlier inequality. Thus $H = G$, so Z generates G. □

5. Multiples of subvarieties

If X is any integral curve, let $\overline{X}$ be the smooth projective curve birational to X, and let g_X be the genus of $\overline{X}$.

Proof of Theorem 1.2. If $\dim X = 0$, then $\dim G = 0$ and we are done. Otherwise Lemma 4.4 lets us reduce to the case where X is an irreducible curve. Let $\tilde{X} \subseteq \overline{X}$ be the normalization of X. By Theorems 1 and 2 of [Ser88], the composition $\tilde{X} \to X \to G$ factors through a generalized Jacobian; i.e., there is a commutative square

$$\begin{array}{ccc} \tilde{X} & \overset{\iota}{\dashrightarrow} & J_{\mathfrak{m}} \\ \downarrow & & \vdots \\ X & \longrightarrow & G \end{array} \qquad \pi$$

where $J_{\mathfrak{m}}$ is the generalized Jacobian of $\overline{X}$ with respect to some modulus $\mathfrak{m}$ supported on $\overline{X} - \tilde{X}$, the morphism ι is the usual one associated to some divisor of degree 1 supported on $\tilde{X}$, and π is a homomorphism. Since X generates G, the homomorphism π must be surjective. The result for $X \hookrightarrow G$ now follows from Lemma 2.1 for $\tilde{X} \to J_{\mathfrak{m}}$. □

The following lemma is more general than what we need to prove Theorem 1.4; we write it this way so that it can be used also in the proof of Theorem 1.8.

Lemma 5.1. *Let $X \to J$ be the usual map from a curve over $\mathbb{F}_q$ to its generalized Jacobian with respect to some modulus $\mathfrak{m}$. Assume that it is an embedding. Let H be a subgroup of $J(\mathbb{F}_q)$, and let $a \in J(\mathbb{F}_q)$. If q is sufficiently large relative to $(J(\mathbb{F}_q) : H)$, g_X, and $\deg \mathfrak{m}$, then $X(\mathbb{F}_q)$ meets $H + a$.*

Proof. Let $A = J/H$. As usual, F will denote a q-power Frobenius endomorphism on A or J. Since H is contained in the kernel of $F - 1$ acting on J, we get the diagonal map ϕ in the following commutative diagram of separable isogenies:

$$\begin{array}{ccc} J & \xrightarrow{F-1} & J \\ \downarrow & \overset{\phi}{\nearrow} & \downarrow \\ A & \xrightarrow[F-1]{} & A. \end{array}$$

The kernel $A(\mathbb{F}_q)$ of the bottom $F-1$ map is mapped by ϕ to the kernel H of the right vertical map. If we define $\psi\colon A \to J$ by $\psi(z) = \phi(z) + a$, then $\psi(A(\mathbb{F}_q)) = H + a$. Let $Y = \psi^{-1}(X)$. By Proposition 10 in [Ser88, I.§2.11], Y is geometrically irreducible. Then g_Y and $\#(\overline{Y} - Y)$ do not depend on a, and are bounded in terms of g, $\deg \mathfrak{m}$, and $\deg \psi = \deg \phi = (J(\mathbb{F}_q) : H)$. Since q is sufficiently large relative to these quantities, the Weil conjectures give $\#Y(\mathbb{F}_q) > 0$. Choose $y \in Y(\mathbb{F}_q)$, and let $x = \psi(y)$. Then $x \in X(\mathbb{F}_q)$ and $x \in \psi(A(\mathbb{F}_q)) = H + a$. □

If G is a commutative algebraic group over $\mathbb{F}_q$ and $m \geq 1$, let $G[m]$ be the kernel of $G(\overline{\mathbb{F}}_q) \xrightarrow{m} G(\overline{\mathbb{F}}_q)$. If $S \subseteq G(\overline{\mathbb{F}}_q)$, let $\mathbb{F}_q(S)$ be the extension of $\mathbb{F}_q$ generated by the coordinates of all the points in S. If $P \in G(\overline{\mathbb{F}}_q)$, let $\mathbb{F}_q(P) = \mathbb{F}_q(\{P\})$.

Proof of Theorem 1.4. We get a square as in the proof of Theorem 1.2. Because G is semiabelian, $\mathrm{Hom}(\mathbb{G}_a, G) = 0$, so we can replace $\mathfrak{m}$ by its associated reduced modulus, and hence $J_{\mathfrak{m}}$ by its quotient by its unipotent radical, in order to assume that $J_{\mathfrak{m}}$ is semiabelian. Thus we reduce to the case where $X \hookrightarrow G$ is the usual inclusion $\iota\colon \overline{X} - \mathfrak{m} \hookrightarrow J_{\mathfrak{m}}$ of a curve with respect to a reduced modulus into its generalized Jacobian.

Let $a \in G(\overline{\mathbb{F}}_q)$. We want to find $n \geq 1$ and $x \in X(\overline{\mathbb{F}}_q)$ such that $nx = a$. Without loss of generality, enlarge q so that X, G, ι, a are all defined over $\mathbb{F}_q$. Choose $m \geq 1$ so that $G(\mathbb{F}_q) \subseteq G[m]$. Since G is semiabelian, $G[m^2]$ is finite. Let $d = [\mathbb{F}_q(G[m^2]) : \mathbb{F}_q]$. Choose $\ell \gg 1$ with $\gcd(\ell, d) = 1$.

If $P \in G(\mathbb{F}_{q^\ell})$ and $mP \in G(\mathbb{F}_q)$, then $m^2 P = 0$, so $P \in G(\mathbb{F}_{q^d})$, and hence $P \in G(\mathbb{F}_{q^\ell}) \cap G(\mathbb{F}_{q^d}) = G(\mathbb{F}_q)$. In other words, $G(\mathbb{F}_{q^\ell})/G(\mathbb{F}_q)$ has order prime to m and hence also to $\#G(\mathbb{F}_q)$. Thus $G(\mathbb{F}_{q^\ell}) \simeq G(\mathbb{F}_q) \times H$.

If $\ell \gg 1$, Lemma 5.1 applied to $\mathbb{F}_{q^\ell}$ gives $x \in X(\mathbb{F}_{q^\ell})$ and $h \in H$ such that $x = h + a$. Choose $n \in \mathbb{Z}_{\geq 1}$ with $n \equiv 1 \pmod{m}$ and $n \equiv 0 \pmod{\#H}$. Then $nx = nh + na = 0 + a = a$. □

Remark 5.2. In the corresponding result of Bogomolov and Tschinkel for curves (Theorem 1 of [BT05]), it is shown that the result remains true if $\bigcup_{n \geq 1} nX(\overline{\mathbb{F}}_q)$ is replaced by $\bigcup_{\substack{n \geq 1 \\ n \equiv 1 \pmod{d}}} nX(\overline{\mathbb{F}}_q)$ for any $d \geq 1$. Our proof gives this as well: when m is chosen in the proof of Theorem 1.4, choose it to be a multiple of d.

This can be generalized to an arbitrary arithmetic progressions:

Corollary 5.3. *Let notation be as in Theorem 1.4, and let $b, d \in \mathbb{Z}_{\geq 1}$. Then*

$$\bigcup_{\substack{n \geq 1 \\ n \equiv b \pmod{d}}} nX(\overline{\mathbb{F}}_q) = G(\overline{\mathbb{F}}_q).$$

Proof. Given $a \in G(\overline{\mathbb{F}}_q)$, choose $a' \in G(\overline{\mathbb{F}}_q)$ with $ba' = a$. Remark 5.2 gives $n' \geq 1$ and $x \in X(\overline{\mathbb{F}}_q)$ with $n' \equiv 1 \pmod{d}$ and $n'x = a'$. Multiply by b to get $bn' \equiv b \pmod{d}$ and $(bn')x = a$. Let $n = bn'$. □

6. Projection

This section proves Theorem 1.8. Throughout this section G is a semiabelian variety over $\overline{\mathbb{F}}_q$, and $X \subseteq G$ is an irreducible subvariety that generates G. As usual, we reduce to the case where X is a curve in a generalized Jacobian. Enlarge q to assume that G and X are defined over $\mathbb{F}_q$. Let F be the q-power Frobenius endomorphism of G. Let $d = \dim G$. Let $\mathcal{P}$ be the set of prime numbers.

Lemma 6.1. *Let $\ell \in \mathcal{P}$. Let $P \in G(\overline{\mathbb{F}}_q)\{\ell\}$. Let $\deg P = [\mathbb{F}_q(P) : \mathbb{F}_q]$. If $\ell \nmid \deg P$, then $\deg P$ divides $\prod_{i=1}^{2d}(\ell^i - 1)$.*

Proof. Let ℓ^s be the order of P. Then $\deg P$ equals the size of the F-orbit of P, which divides the order of the image of F in $\operatorname{Aut} G[\ell^s]$, which divides $\#\operatorname{Aut} G[\ell^s]$, which divides $\#\operatorname{GL}_{2d}(\mathbb{Z}/\ell^s\mathbb{Z})$ (since $G[\ell^s]$ is a free $\mathbb{Z}/\ell^s\mathbb{Z}$-module of rank $\leq 2d$), and $\#\operatorname{GL}_{2d}(\mathbb{Z}/\ell^s\mathbb{Z})$ is a power of ℓ times $\prod_{i=1}^{2d}(\ell^i - 1)$. Finally, $\gcd(\deg P, \ell) = 1$. □

If $r \in \mathcal{P}$, let $\mathbb{F}_{q^{r^\infty}} = \bigcup_{i \geq 0} \mathbb{F}_{q^{r^i}}$.

Lemma 6.2. *If $S \subseteq \mathcal{P}$ is finite and $r \in \mathcal{P} - S$, then $G(\mathbb{F}_{q^{r^\infty}})\{S\}$ is finite.*

Proof. It suffices to consider $S = \{\ell\}$ for a single prime $\ell \neq r$. By Lemma 6.1, the degrees of points in $G(\mathbb{F}_{q^{r^\infty}})\{\ell\}$ are bounded, say by N. Then $G(\mathbb{F}_{q^{r^\infty}})\{\ell\} \subseteq \bigcup_{n=1}^{N} G(\mathbb{F}_{q^n})$, which is finite. □

If $T \subseteq \mathcal{P}$, define the *upper density of T* as

$$\overline{\mu}(T) = \limsup_{x \to \infty} \frac{\#\{\ell \in T : \ell \leq x\}}{\#\{\ell \in \mathcal{P} : \ell \leq x\}}.$$

Define $\underline{\mu}(T)$ similarly using $\liminf$ instead of $\limsup$. If $\overline{\mu}(T) = \underline{\mu}(T)$, let $\mu(T)$ be the common value, and call it the *density of T*. Also define

$$\eta(T) = \sup_{x \in \mathbb{Z}_{\geq 1}} \frac{\#\{\ell \in T : \ell \leq x\}}{\#\{\ell \in \mathcal{P} : \ell \leq x\}}.$$

Thus $\overline{\mu}(T) \leq \eta(T)$.

Lemma 6.3. *Let r be prime. Then the set $T := \{\ell \in \mathcal{P} : (\exists n \geq 0)$ such that $\ell \mid \#G(\mathbb{F}_{q^{r^n}})\}$ has density 0.*

Proof. For $m \geq 1$, let T_m be the subset of T obtained by discarding r (if it is in T) and all primes dividing $\#G(\mathbb{F}_{q^{r^m}})$. Since only finitely many primes were discarded, $\overline{\mu}(T) = \overline{\mu}(T_m)$.

Suppose $\ell \in T_m$. Then there is a point in $G(\mathbb{F}_{q^{r^\infty}})\{\ell\}$ of degree r^n for some $n > m$, so Lemma 6.1 gives

$$r^m \mid r^n \mid \prod_{i=1}^{2d} (\ell^i - 1).$$

Factor the right hand side as a polynomial in $\overline{\mathbb{Q}}[\ell]$ into $\prod_{j=1}^{s}(\ell - \zeta_j)$ where $s = 1+2+\cdots+2d$ and each ζ_j is in $\overline{\mathbb{Q}}$. Extend the r-adic valuation on $\mathbb{Q}$ to $v_r \colon \overline{\mathbb{Q}}^\times \to \mathbb{Q}$ with $v(r) = 1$. Then $\ell \in T_m$ implies $v_r(\ell - \zeta_j) \geq m/s$ for some j. The set of integers ℓ satisfying $v_r(\ell - \zeta_j) \geq m/s$ for a particular j is either empty or a residue class modulo $r^{\lceil m/s \rceil}$, so T_m is contained in a union of at most s residue classes modulo $r^{\lceil m/s \rceil}$. Dirichlet's theorem on primes in arithmetic progressions says that the set of primes in each residue class has density $1/\left(r^{\lceil m/s \rceil}(1 - r^{-1})\right)$. Thus

$$\overline{\mu}(T) = \overline{\mu}(T_m) \leq \frac{s}{r^{\lceil m/s \rceil}(1 - r^{-1})} \to 0$$

as $m \to \infty$. □

Lemma 6.4. *Given $a \in G(\overline{\mathbb{F}}_q)$, $\epsilon > 0$, and a finite set $S_0 \subseteq \mathcal{P}$, there exists a finite set $U \subseteq \mathcal{P} - S_0$ with $\eta(U) < \epsilon$ and $a \in X(\overline{\mathbb{F}}_q) + G(\overline{\mathbb{F}}_q)\{U\}$.*

Proof. Enlarge q to assume $a \in A(\mathbb{F}_q)$. Pick $r \in \mathcal{P} - S_0$ with $1/\pi(r) < \epsilon$, where $\pi(r)$ is the number of primes $\leq r$. The set T defined in Lemma 6.3 satisfies $\overline{\mu}(T) = 0$. Define subsets $\tau := \{\ell \in T : \ell \leq t\} - \{r\}$ and $T' := T - \tau$ depending on a parameter $t > 0$. As $t \to \infty$ we have

$$\eta(T') \leq \eta(\{r\}) + \eta(T' - \{r\}) \longrightarrow \eta(\{r\}) + \overline{\mu}(T) = \frac{1}{\pi(r)} + 0 < \epsilon$$

so we can choose $t > \max S_0$ such that $\eta(T') < \epsilon$. Let $B = \#G(\mathbb{F}_{q^{r^\infty}})\{\tau\}$, which is finite by Lemma 6.2 since $r \notin \tau$. For all n, the subgroup $H := G(\mathbb{F}_{q^{r^n}})\{T'\}$ of $G(\mathbb{F}_{q^{r^n}})$ has index $\#G(\mathbb{F}_{q^{r^n}})\{\tau\}$, which is bounded by B. By Lemma 5.1, if $n \gg 1$, then $X(\mathbb{F}_{q^{r^n}})$ meets $H + a$. Then $a = x - h$ for some $x \in X(\mathbb{F}_{q^{r^n}})$ and $h \in H$. Let U be the (finite) set of primes dividing the order of h. Then $U \subseteq T' \subseteq \mathcal{P} - S_0$, since $t > \max S_0$ and $r \notin S_0$. Now $a = x - h \in X(\overline{\mathbb{F}}_q) + G(\overline{\mathbb{F}}_q)\{U\}$, and $\eta(U) \leq \eta(T') < \epsilon$. □

Lemma 6.5. *For $i \geq 1$, let $U_i \subseteq \mathcal{P}$ be finite. If $\sum \eta(U_i)$ converges, then $\mu\left(\bigcup U_i\right) = 0$.*

Proof. The definitions imply

$$\overline{\mu}\left(\bigcup U_i\right) = \overline{\mu}\left(\bigcup_{i \geq N} U_i\right) \leq \eta\left(\bigcup_{i \geq N} U_i\right) \leq \sum_{i \geq N} \eta(U_i) \to 0$$

as $N \to \infty$. □

Lemma 6.6. *Given a finite set $S_0 \subseteq \mathcal{P}$, there exists $U \subseteq \mathcal{P} - S_0$ of density 0 such that $X(\overline{\mathbb{F}}_q) + G(\overline{\mathbb{F}}_q)\{U\} = G(\overline{\mathbb{F}}_q)$.*

Proof. Let $a_1, a_2, \ldots$ be an enumeration of $A(\overline{\mathbb{F}}_q)$. Let U_i be as in Lemma 6.4 for $a = a_i$ and $\epsilon = 2^{-i}$ and S_0. By Lemma 6.5, $U := \bigcup U_i$ has density 0. Each U_i is disjoint from S_0, so U is disjoint from S_0. By construction,

$$a_i \in X(\overline{\mathbb{F}}_q) + G(\overline{\mathbb{F}}_q)\{U_i\} \subseteq X(\overline{\mathbb{F}}_q) + G(\overline{\mathbb{F}}_q)\{U\}$$

for all i. □

Proof of Theorem 1.8. Let $S = \mathcal{P} - U$ where U is as in Lemma 6.6. □

Acknowledgements

I thank Yuri Tschinkel for pointing out the reference [PS03] and for pointing out that my notation in an earlier draft was ambiguous at one point.

References

[AI85] Greg W. Anderson and Robert Indik, *On primes of degree one in function fields*, Proc. Amer. Math. Soc. **94** (1985), no. 1, 31–32. MR781050 (86h:11107)

[BT03] Fedor Bogomolov and Yuri Tschinkel, *Rational curves and points on K3 surfaces*, 2003. Preprint, `arXiv:math.AG/0310254` .

[BT05] ———, *Curves in abelian varieties over finite fields*, Int. Math. Res. Not. **4** (2005), 233–238. MR2128435

[dJ96] A. J. de Jong, *Smoothness, semi-stability and alterations*, Inst. Hautes Études Sci. Publ. Math. **83** (1996), 51–93. MR1423020 (98e:14011)

[Poo04] Bjorn Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127. MR2144974 (2006a:14035)

[PS03] Florian Pop and Mohamed Saïdi, *On the specialization homomorphism of fundamental groups of curves in positive characteristic*, Galois groups and fundamental groups, 2003, pp. 107–118. MR2012214 (2004i:14024)

[Ser88] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988. Translated from the French. MR918564 (88i:14041)

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `poonen@math.berkeley.edu`
URL: `http://math.berkeley.edu/~poonen`