

Uniform potential density for rational points on algebraic groups and elliptic K3 surfaces

Kuan-Wen Lai

Masahiro Nakahara

Abstract

A collection of varieties satisfies uniform potential density if each of them contains a dense subset of rational points after extending its ground field by a bounded degree. In this paper, we prove that uniform potential density holds for connected algebraic groups of a fixed dimension over fields of characteristic zero as well as elliptic K3 surfaces over number fields.

Contents

1	Introduction	2
2	Finite subgroups of general linear groups	4
3	Uniform potential density for algebraic groups	6
3.1	Genus one curves versus elliptic curves	6
3.2	Abelian varieties of higher dimensions	9
3.3	Algebraic groups and their torsors	12
4	Uniform potential density for elliptic K3 surfaces	19
4.1	Picard groups and automorphisms	19
4.2	Jacobian fibrations and rational multisections	23
4.3	Proof of uniform potential density	29
5	Brauer groups and uniform potential density	32
5.1	Brauer–Manin obstructions and related conjectures	32
5.2	A sufficient condition for uniform potential density	33

1 Introduction

A variety X over a field k satisfies *potential density* if there exists a finite extension L/k such that the set of L -rational points $X(L)$ is Zariski dense. For example, abelian varieties over number fields satisfy potential density [HT00, Proposition 3.1], while rational points do not have to be dense over the original field. Bogomolov and Tschinkel [BT00] proved potential density for K3 surfaces X over number fields with an elliptic fibration, though it is not known whether $X(k)$ is dense as soon as it is non-empty. In this paper, we consider whether the degree of the extension L/k can be taken uniformly with respect to the geometric properties of X :

Definition 1.1. A collection \mathcal{C} of varieties satisfies *uniform potential density* if there exists a constant $d_{\mathcal{C}}$ such that for any $X/k \in \mathcal{C}$, there exists a finite extension L/k of degree bounded by $d_{\mathcal{C}}$ such that $X(L)$ is Zariski dense.

We allow the members in \mathcal{C} to have different ground fields k . Also, the constant $d_{\mathcal{C}}$ is independent of the ground field. Examples of collections of varieties that satisfy uniform potential density include smooth curves of genus zero (they can be realized as plane conics and so the rational points are dense after a quadratic extension), del Pezzo surfaces (see Proposition 2.3), and torsors under simple linear algebraic groups of a fixed dimension [Tit92]. Our first main theorem is based on the last example:

Theorem 1.2. *Uniform potential density holds for*

- *the collection of torsors under connected linear algebraic groups of a fixed dimension over infinite perfect fields;*
- *the collection of connected algebraic groups of a fixed dimension over fields of characteristic zero.*

In particular, the second part of the theorem implies that uniform potential density holds for abelian varieties of a fixed dimension. We also compute an explicit bound $d_{\mathcal{C}}$ for the degree of the field extension in the case of abelian varieties (see Theorem 3.10). To prove Theorem 1.2, we use Chevalley’s structure theorem to divide the problem into two parts: uniform potential density for (1) abelian varieties (Corollary 3.11), and for (2) torsors under connected linear algebraic groups (Corollary 3.18). For abelian varieties, we use Zarhin’s trick to first embed an abelian variety into a projective space with bounded degree. Then we use the Mordell–Lang conjecture to construct a non-torsion point over a bounded extension of the ground field. From there we use an inductive argument while keeping track of degrees of extensions to construct a rational point that generates a dense subgroup.

For torsors under connected linear algebraic groups, we start with a result of [Tit92] that concerns the splitting fields of geometrically almost simple groups. More precisely, he showed that the degree of field extension to make such a group split can be taken to divide an integer that depends only the type of the group. We then show that one can deduce the uniform potential density for torsors under geometrically almost simple groups, and then to semisimple groups, and finally to connected linear algebraic groups.

Our second main theorem extends the result for elliptic K3 surfaces by Bogomolov and Tschinkel [BT00].

Theorem 1.3. *Uniform potential density holds for the collection of elliptic K3 surfaces over number fields.*

By an elliptic K3 surface, we mean a K3 surface together with a morphism $X \rightarrow \mathbb{P}^1$ whose generic fiber is a smooth curve of genus one over the function field $k(\mathbb{P}^1)$. Note that the analogous statement for curves of genus one fails (Proposition 3.1). We also compute explicitly the constant d_C that one can take for potential density to hold. See Theorem 4.14 for details. Our proof of Theorem 1.3 follows that of potential density in [BT00]. While some of their constructions can be done over the ground field, others require an extension whose degree is unknown. We begin by using a result of [Min87] on finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ to show that the geometric Néron–Severi group can be defined over a bounded extension of the ground field. The key problem is then to bound the degree of the field of definition of an elliptic or rational multisection which is used to produce rational points. This is done using lattice theory in Lemma 4.12.

Theorem 1.3 provides an evidence to the following conjectures in the case of K3 surfaces: let $\mathcal{C} = \{(X, k)\}$ be a collection of smooth and geometrically integral varieties X over number fields k . Let $\mathrm{Br}(X)$ denote the Brauer group of X and define

$$\mathrm{Br}_0(X) := \mathrm{im}(\mathrm{Br}(k) \longrightarrow \mathrm{Br}(X)).$$

We say \mathcal{C} satisfies

- *uniform boundedness of exponent for Brauer groups (UBEB)* if, for every integer $d > 0$, there exists a constant c_d such that $c_d \alpha = 0$ for any $\alpha \in \mathrm{Br}(X_L)/\mathrm{Br}_0(X_L)$ where $X/k \in \mathcal{C}$ and L/k is an extension such that $[L : k] \leq d$;
- *Brauer–Manin obstruction is the only one to weak approximation (BMWA)* if for any $X/k \in \mathcal{C}$ and finite extension L/k , we have $X(L)$ dense in $X(\mathbb{A}_L)^{\mathrm{Br}}$.
- *uniform potential local solubility (UPLS)* if, there exists a constant c such that for any $X/k \in \mathcal{C}$, there exists an extension L/k of degree $\leq c$ such that X_L is everywhere locally soluble.

Theorem 1.4. *Let \mathcal{C} be a collection of smooth projective geometrically integral varieties X/k over number fields such that $H^1(X, \mathcal{O}_X) = 0$ and $\mathrm{Pic}(X_{\bar{k}})$ is torsion-free of bounded rank. If \mathcal{C} satisfies UBEB, BMWA, and UPLS then it also satisfies uniform potential density.*

For K3 surfaces over number fields, both UBEB and BMWA are conjectures [VA17, Sko09], see §5 for a discussion. It would follow from these conjectures that uniform potential density holds for all K3 surfaces over number fields provided that UPLS holds. Our Theorem 1.3 can be taken as further evidence toward these conjectures.

Organization of the paper. In §2, we recall a result due to Minkowski which plays a fundamental role in proving the main theorems and discuss the uniform potential density

for del Pezzo surfaces. We prove uniform potential density for algebraic groups in §3 and for elliptic K3 surfaces in §4. The relationship between uniform potential density and the Brauer–Manin obstruction is discussed in §5.

Acknowledgements. We thank Zinovy Reichstein for his kind help for dealing with the case of algebraic groups, and thank Brendan Hassett for his suggestion on improving the proof of the case of elliptic K3 surfaces. We also thank Daniel Loughran for suggesting us including del Pezzo surfaces for uniform potential density and for his comments on the first draft of the paper. We would also like to thank the referees for correcting errors in earlier versions of the paper and giving suggestions on improving the expositions. The second author was sponsored by EPSRC grant EP/R021422/2.

2 Finite subgroups of general linear groups

We begin with the following well-known result due to Minkowski.

Theorem 2.1 ([Min87]). *For every positive integer n , there are only finitely many isomorphism classes of finite subgroups in $\mathrm{GL}(n, \mathbb{Z})$.*

See also [KP02] for a discussion on this theorem. Motivated by this result, we make the following convenient notation which will be used throughout the paper.

Definition 2.2. For every positive integer n , we define \mathbf{c}_n to be the maximal cardinality among the cardinalities of the finite subgroups in $\mathrm{GL}(n, \mathbb{Z})$.

Notice that the constant \mathbf{c}_n increases as n increases since $\mathrm{GL}(n, \mathbb{Z})$ is a subgroup of $\mathrm{GL}(n+1, \mathbb{Z})$. Theorem 2.1 will be critical in proving uniform potential density for many cases later on. As a quick application, we prove that del Pezzo surfaces satisfy uniform potential density. If X is a del Pezzo surface of degree $1 \leq d \leq 7$, then the Galois action on $\mathrm{Pic}(X_{k^s}) \simeq \mathbb{Z}^{10-d}$ gives rise to a homomorphism

$$\mathrm{Gal}(k^s/k) \longrightarrow \mathrm{GL}(10-d, \mathbb{Z}). \quad (2.1)$$

Because the Picard group is generated by the finitely many (-1) -curves on X_{k^s} , there exists a finite extension L/k such that $\mathrm{Pic}(X_L) = \mathrm{Pic}(X_{k^s})$ and $\mathrm{Gal}(k^s/L)$ appears as the kernel of (2.1). In particular, the group $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(k^s/k) / \mathrm{Gal}(k^s/L)$ is isomorphic to a subgroup of $\mathrm{GL}(10-d, \mathbb{Z})$. Thus

$$[L : k] = |\mathrm{Gal}(L/k)| \leq \mathbf{c}_{10-d} \leq \mathbf{c}_9.$$

The condition $\mathrm{Pic}(X_L) = \mathrm{Pic}(X_{k^s})$ implies that every (-1) -curve of X_{k^s} is defined over L . Contracting part of them gives a birational morphism $X_L \rightarrow \mathbb{P}_L^2$, whose inverse produces a dense subset of rational points on X_L .

Using the known properties of del Pezzo surfaces however, the bound for the degree L/k in which we get a dense set of rational points can be vastly improved from \mathbf{c}_9 .

Proposition 2.3. *For a del Pezzo surface X of degree $1 \leq d \leq 9$ over an infinite field k , we can obtain a Zariski dense subset of rational points by passing to a finite extension L/k of degree bounded by a number depending only on d as listed below:*

d	1	2	3	4	5	6	7	8	9
$[L : k] \leq$	$240 \cdot 4$	4	3	4	1	6	1	2	3

Proof. We divide the proof into cases based on d .

Case $d = 9$: in this case, X is a Sever–Brauer surface, which corresponds to (the isomorphism class of) a central simple algebra A of degree 3 [GS17, Theorem 5.2.1]. By Wedderburn’s theorem (see, e.g., [GS17, Theorem 2.1.3]), A is isomorphic to a matrix ring $M_n(D)$ for some $n \geq 1$ and some division algebra D . Notice that the degree of D divides 3 in our situation. By [GS17, Theorem 2.2.7], the algebra D , and thus A , admits a splitting field L/k of degree at most 3. It follows that $X_L \cong \mathbb{P}_L^2$ and so $X(L)$ is dense.

Case $d = 8$: there are two possibilities, X is isomorphic to either a blow up of \mathbb{P}^2 at a point or a quadric surface. In the former case X is birational to \mathbb{P}^2 . In the latter case, we can find a rational point on X by taking a quadratic extension L/k , in which case the stereographic projection from the point maps X_L birationally onto \mathbb{P}_L^2 .

Case $d = 5, 7$: $X(k)$ is dense since X is birational to \mathbb{P}^2 , see [VA13, Theorem 2.1].

Case $d = 6$: there are a total of six (-1) -curves on X_{k^s} , so one of them is defined over an extension L/k of degree at most 6. Contracting this (-1) -curve gives a del Pezzo surface of degree 7 over L , which shows $X(L)$ is dense by Case $d = 7$.

Case $d = 4$: if X has a rational point, then it is unirational and thus contains a dense subset of rational points [Pie12, Proposition 5.19]. Since X is isomorphic to the intersection of two quadrics in \mathbb{P}^4 , it has a point of degree at most 4.

Case $d = 3$: the situation is the same as $d = 4$, namely, the existence of a rational point is sufficient [Kol02, Theorem 1.1]. In this case, X is isomorphic to a cubic surface in \mathbb{P}^3 , so the bound can be taken as 3.

Case $d = 2$: the linear system $| -K_X |$ defines a double cover $X \rightarrow \mathbb{P}^2$, so there exists a rational point over a quadratic extension L/k . By [STVA14, Corollary 1.3], X_L becomes unirational over a further quadratic extension L'/L , so the bound in this case is 4.

Case $d = 1$: the number of (-1) -curves on X_{k^s} equals 240, so there is an extension L/k of degree at most 240 where one of them is defined over L . Contracting this (-1) -curve gives a degree 2 del Pezzo surface over L . By Case $d = 2$, we can get a dense set of rational points over a further extension L'/L of degree at most 4. \square

Remark 2.4. If $\text{char}(k) \neq 2, 3$, the bound for $d = 1$ in Proposition 2.3 can be slightly improved to 240. To see this, first recall that the linear system $| -K_X |$ induces an elliptic fibration $\mathcal{E} \rightarrow \mathbb{P}^1$ with a section. When $\text{char}(k) \neq 2, 3$, the linear system $| -3K_X |$ embeds X into the weighted projective space $\mathbb{P}(2, 3, 1, 1)$ with coordinates x, y, z, w as a sextic hypersurface $y^2 = x^3 + f(z, w)x + g(z, w)$, where the fibration \mathcal{E} is given explicitly by the projection (see, e.g., [VA13, §1.5.4] or [SvL14, §1])

$$\mathbb{P}(2, 3, 1, 1) \dashrightarrow \mathbb{P}^1 : [x : y : z : w] \mapsto [z : w].$$

Under this model, Salgado and van Luijk proved that all the (-1) -curves on $X_{k,s}$ appear as sections of $\mathcal{E}_{k,s}$ [SvL14, Lemma 2.2] and none of them is torsion [SvL14, Theorem 6.4]. Let L/k be an extension of degree at most 240 over which one of the (-1) -curves C is defined. Then the orbit of C under the group law of the generic fiber produces a dense subset of sections and thus a dense subset of rational points.

3 Uniform potential density for algebraic groups

In this section, we establish uniform potential density for connected algebraic groups over fields of characteristic zero. We start by studying basic properties about rational points on elliptic curves, then use it to establish uniform potential density for abelian varieties. We then prove uniform potential density for torsors under connected linear algebraic groups. We finish proof of Theorem 1.2 by combining these two results via Chevalley’s structure theorem.

Most of the results in this section are proved over fields of characteristic zero, but some statements hold over more general fields.

3.1 Genus one curves versus elliptic curves

Uniform potential density fails for curves of genus one, however, it holds for elliptic curves, that is, genus one curves that contains a rational point. Let us explain these two facts below.

Proposition 3.1. *The collection of genus one curves over number fields does not satisfy uniform potential density.*

Proof. Fix an elliptic curve E over a number field k . Recall that the genus one curves over k which are isomorphic to E over the algebraic closure \bar{k} are classified by the Weil–Châtelet group $H^1(k, E)$.¹ For every genus one curve C over k , its index i_C is defined as the greatest common divisor of the degrees of closed points on C . It is well known that $H^1(k, E)$ is torsion and that the order of $[C] \in H^1(k, E)$ divides i_C .

For any integer n , the Kummer sequence of $\text{Gal}(\bar{k}/k)$ -modules

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{\times n} E \longrightarrow 0$$

induces the exact sequence

$$E(k)/nE(k) \longrightarrow H^1(k, E[n]) \longrightarrow H^1(k, E)[n]$$

The group $H^1(k, E[n])$ is infinite. (See Lemma 4.6.) Since $E(k)/nE(k)$ is finite by the weak Mordell–Weil theorem [Sil09, VIII, Theorem 6.7], the group $H^1(k, E)[n]$ is infinite. In particular, there exists $[C] \in H^1(k, E)$ of arbitrarily large prime order and so arbitrarily

¹(Updated on December 7, 2021) This sentence should be corrected as “Recall that *torsors under E* are classified by the Weil–Châtelet group $H^1(k, E)$.”.

large index. Such a curve C does not have rational points over fields of degree smaller than the index over k . Thus the collection of genus one curves does not satisfy uniform potential density. \square

Given an abelian group G and a subgroup H , we define the saturation of H (in G) to be

$$\{g \in G : \text{there exists } n \in \mathbb{Z} \text{ such that } ng \in H\}.$$

Uniform potential density for elliptic curves over number fields can be derived from the following more general statement:

Theorem 3.2. *Let E be an elliptic curve over a field k of characteristic 0. Suppose that $\Gamma \subset E(\bar{k})$ is a finitely generated subgroup and let $\Gamma_0 \subset E(\bar{k})$ be its saturation. Then there exists an extension L/k of degree at most 18 such that $E(L) \not\subset \Gamma_0$. Moreover, if k is a number field, the degree bound can be improved to 2.*

Our approaches over number fields and over fields of characteristic zero are different. Let us start with the case of number fields. The general case will be proved later.

Proof of Theorem 3.2 over number fields. Because Γ is finitely generated, there exists a finite extension L_0/k such that Γ_0 is contained in the saturation of $E(L_0)$.

Let O be the origin of E and let $f: E \rightarrow \mathbb{P}^1$ be the double cover defined by $|2O|$. By Hilbert's irreducibility theorem, for any finite extension L/k , there exists infinitely many $x \in \mathbb{P}^1(k)$ such that the fiber $f^{-1}(x)$ is irreducible of degree 2 over L . Using this fact, we can inductively produce a list of k -rational points $\{x_1, x_2, x_3, \dots\} \subset \mathbb{P}^1(k)$ such that the splitting fields L_i of the fibers $f^{-1}(x_i)$ satisfy the property:

For every integer $i \geq 1$, the fiber $f^{-1}(x_i)$ is irreducible over the composite field $L_0 L_1 \cdots L_{i-1}$.

As each L_i/k , $i \geq 1$, is a quadratic extension, it follows that $L_i \cap L_j = k$ whenever $i, j \geq 0$ are distinct.

For each $x_i \in \mathbb{P}^1(k)$, the fiber $f^{-1}(x_i)$ splits into two points y_i, y'_i over L_i such that $y_i = -y'_i$ in the group law of E . Note that y_i and y'_i are $\text{Gal}(\bar{k}/k)$ -conjugates. Suppose $y_i \in \Gamma_0$. Then there exists $n > 0$ such that $ny_i \in E(L_0)$. Because ny_i is defined over L_i and $L_i \cap L_0 = k$, the point ny_i is in fact defined over k . Since ny_i and ny'_i are $\text{Gal}(\bar{k}/k)$ -conjugates, this implies $ny_i = ny'_i$ and thus $2ny_i = 0$. In particular, $y_i \in E(L_i)_{\text{tor}}$. By Merel's theorem (see, e.g., [Sil09, VIII, Theorem 7.5.1]), there exists an integer N such that $|E(L)_{\text{tor}}| \leq N$ for any quadratic extension L/k . In particular, every point in $E(L_i)_{\text{tor}}$ where $i \geq 1$ has order at most N . It follows that

$$\bigcup_{i \in \mathbb{N}} E(L_i)_{\text{tor}} \subset E(\bar{k})[N!] \tag{3.1}$$

where $E(\bar{k})[N!]$ is the finite set of torsion \bar{k} -points of order dividing $N!$. If $y_i \in \Gamma_0$ for infinitely many $i \in \mathbb{N}$, we would obtain infinitely many points on the left hand side of (3.1), which is impossible. Therefore, all but finitely many y_i are not in Γ_0 . Hence all but finitely many of the quadratic extensions L_i/k satisfies $E(L_i) \not\subset \Gamma_0$. \square

Proof of Theorem 3.2 in the general case. Let us consider the abelian surface $X := E \times E$ and the divisor $D := E \times \{0\} + \{0\} \times E$ on X . Note that $D^2 = 2$, so D is ample by [Kan94, Corollary 2.2]. This implies that $3D$ is very ample [EvdGM20, (2.26)], so we can embed X into \mathbb{P}^n as a subvariety of degree $(3D)^2 = 18$. Bertini's theorem guarantees the existence of a smooth sectional curve $C \subset X$ of degree 18. One can compute that C has genus 10 by the adjunction formula.

Define $\Lambda_0 := \Gamma_0 \times \Gamma_0 \subset X(\bar{k})$. According to the Mordell–Lang conjecture (see, e.g., [Maz00] and the references cited there), the intersection $C \cap \Lambda_0$ contains only finitely many points. It follows that, among the infinitely many closed points of degree at most 18 on C cut out by hyperplanes defined over k , there exists at least one not in Λ_0 . As a result, there exists an extension L/k of degree at most 18 such that $X_L \cong E_L \times E_L$ has an L -rational point $p \notin \Lambda_0$. By projecting p to one of the copies of E_L , we obtain an L -rational point on E_L not lying in Γ_0 . \square

Theorem 3.2 has an immediate consequence for uniform potential density for elliptic curves, which is well-known to experts but we include the corollary here for completeness.

Corollary 3.3. *Let E be an elliptic curve over a field k of characteristic zero. Then there exists an extension L/k of degree bounded by 18 such that $E(L)$ contains a non-torsion point and thus is Zariski dense in E_L . The bound 18 can be improved to 2 if k is a number field. As a consequence, the collection of elliptic curves over fields of characteristic zero satisfies uniform potential density.*

Proof. Applying Theorem 3.2 with $\Gamma = \{0\}$, one obtains $p \in E(L)$ not lying in Γ_0 for an extension L/k of degree bounded by 2 in the number field case and by 18 in general. Because Γ_0 contains all torsion points of $E(\bar{k})$, the point p is non-torsion. Hence it generates a subset $\{np \mid n \in \mathbb{Z}\} \subset E(L)$ Zariski dense in E_L . \square

Let us introduce another corollary of Theorem 3.2. Recall that an elliptic surface $\mathcal{E} \rightarrow C$ over a field k *splits* if there exist an elliptic curve E_0 over k and a birational map between elliptic fibrations $\mathcal{E} \xrightarrow{\sim} E_0 \times C$. Suppose that \mathcal{E} does *not* split. Then the group $E(k(C))$ is finitely generated by the Mordell–Weil theorem for function fields [Sil94, III, Theorem 6.1].

Corollary 3.4. *Suppose that E is an elliptic curve over k , where k is*

- *a number field, or*
- *the function field of a curve C over a field of characteristic 0 such that the associated elliptic surface $\mathcal{E} \rightarrow C$ does not split.*

Then there is an extension L/k of degree at most 2 in the number field case and at most 18 in the function field case such that $\text{rk}(E(L)) > \text{rk}(E(k))$.

Proof. By the Mordell–Weil theorem for number fields or for function fields, where the latter requires $\mathcal{E} \rightarrow C$ to be non-split, the group $E(k)$ is finitely generated. Applying Theorem 3.2 with $\Gamma = E(k)$, we conclude that there exists an extension L/k and $p \in E(L)$ such that

$p \notin \Gamma_0$. Moreover, the degree of L/k can be taken to be at most 2 in the number field case and at most 18 in the function field case. Since p does not lie in the saturation of $E(k)$, we have $\text{rk}(E(L)) > \text{rk}(E(k))$. \square

3.2 Abelian varieties of higher dimensions

Our proof of uniform potential density for abelian varieties over a fixed dimension, follows the main ideas for potential density in [HT00, Proposition 3.1].

3.2.1 Existence of a non-torsion point

Lemma 3.5. *Let X be a principally polarized abelian variety of dimension n over a field k . Then X admits a very ample line bundle \mathcal{D} that embeds X as a subvariety in \mathbb{P}^{2^n-1} of degree $6^n(n!)$.*

Proof. For every $\mathcal{E} \in \text{Pic}(X_{\bar{k}})$, we will denote by $\varphi_{\mathcal{E}}$ the isogeny

$$\varphi_{\mathcal{E}}: X \longrightarrow X^{\vee}, \quad x \longmapsto t_x^* \mathcal{E} \otimes \mathcal{E}^{-1}$$

where t_x is the translation by x . Let $\lambda: X \longrightarrow X^{\vee}$ be a principal polarization and \mathcal{P} be the Poincaré bundle on $X \times X^{\vee}$. Then there exists $\mathcal{L} \in \text{Pic}(X_{\bar{k}})$ such that $\lambda = \varphi_{\mathcal{L}}$. Moreover, the line bundle $\mathcal{D} := (\text{id}_X, \lambda)^* \mathcal{P} \in \text{Pic}(X)$ is ample and satisfies [EvdGM20, Proposition 11.1]

$$\varphi_{\mathcal{D}} = 2\lambda = 2\varphi_{\mathcal{L}} \in \text{Hom}^{\text{Sym}}(X, X^{\vee}).$$

Using the exact sequence $0 \rightarrow X^{\vee}(k) \rightarrow \text{Pic}(X) \xrightarrow{\varphi} \text{Hom}^{\text{Sym}}(X, X^{\vee})$, we conclude that

$$\mathcal{D} = \mathcal{L}^{\otimes 2} \otimes \mathcal{N} \tag{3.2}$$

for some $\mathcal{N} \in \text{Pic}^0(X) = X^{\vee}(k)$.

The line bundle $3\mathcal{D}$ is very ample as \mathcal{D} is ample [EvdGM20, (2.26)] and thus defines an embedding $X \hookrightarrow \mathbb{P}^{\ell}$. To compute the degree of X in \mathbb{P}^{ℓ} , we use (3.2) and the Riemann–Roch formula for abelian varieties to get

$$\chi(\mathcal{D}) = c_1(\mathcal{D})^n/n! = (2c_1(\mathcal{L}) + c_1(\mathcal{N}))^n/n!. \tag{3.3}$$

We have $c_1(\mathcal{N}) = 0$ and also $c_1(\mathcal{L})^n/n! = \chi(\mathcal{L}) = \sqrt{\deg \lambda} = 1$. Plugging these into (3.3), we obtain $\chi(\mathcal{D}) = 2^n$. Therefore, \mathcal{D} embeds X into \mathbb{P}^{2^n-1} with degree given by

$$\deg(X) = (3c_1(\mathcal{D}))^n = 3^n \chi(\mathcal{D})(n!) = 3^n 2^n (n!) = 6^n (n!).$$

\square

The following lemma is an analog of Theorem 3.2 for abelian varieties.

Lemma 3.6. *Let A be an abelian variety of dimension $g \geq 2$ over a field k of characteristic zero. Suppose that $\Gamma \subset A(\bar{k})$ is a finitely generated subgroup and let Γ_0 be its saturation. Then there exists an extension L/k of degree at most $6^{8g} \cdot (8g)!$ such that $A(L) \not\subset \Gamma_0$.*

Proof. Fix an isogeny $\varphi: A \rightarrow A^\vee$ and define $X := A^4 \times (A^\vee)^4$. Consider the finitely generated subgroup

$$\Gamma_X := \Gamma_0^4 \times \varphi(\Gamma_0)^4 \subset X(\bar{k}).$$

and denote by $(\Gamma_X)_0 \subset X(\bar{k})$ its saturation. Let us first prove that there exists a finite extension L/k of degree at most $6^{8g} \cdot (8g)!$ such that $X(L) \not\subset (\Gamma_X)_0$. In the case that X contains an elliptic curve E as a subgroup over k , we can apply Theorem 3.2 to E and the subgroup $E(\bar{k}) \cap (\Gamma_X)_0$. This gives us an extension L/k of degree at most $18 < 6^{8g} \cdot (8g)!$ such that $E(L)$ is not contained in the saturation of $E(\bar{k}) \cap (\Gamma_X)_0$ in $E(\bar{k})$, which implies that $X(L) \not\subset (\Gamma_X)_0$, as desired. Therefore, we assume that X does not contain an elliptic curve over k below.

Due to Zarhin's trick [EvdGM20, Theorem 11.29], the product $X = A^4 \times (A^\vee)^4$ admits a principal polarization. Note that X has dimension $8g$, so Lemma 3.5 implies that X can be realized as a projective variety of degree $6^{8g} \cdot (8g)!$. Let us cut X with hyperplanes over k subsequently to get a curve $C \subset X$, which has genus at least 2 since X contains no elliptic curve by hypothesis. Moreover, we may assume that C is smooth and passes through the origin of X due to Bertini's theorem. In this setting, the intersection $C(\bar{k}) \cap (\Gamma_X)_0$ is finite due to the Mordell–Lang conjecture. (See, e.g., [Maz00].) On the other hand, we can obtain infinitely many points on C of degrees at most $\deg(C) = 6^{8g} \cdot (8g)!$ by further cutting C with hyperplanes over k . Hence there exists a point $p \in C$ not in $(\Gamma_X)_0$ whose residue field $L := k(p)$ satisfies $[L : k] \leq 6^{8g} \cdot (8g)!$. In particular, $X(L) \not\subset (\Gamma_X)_0$.

Finally, take any $p \in X(L)$ not lying in $(\Gamma_X)_0$. If all the projections $X \rightarrow A$ and $X \rightarrow A^\vee$ map p to Γ_0 and $\varphi(\Gamma_0)$, respectively, then p belongs to Γ_X , a contradiction. Hence there exists a projection $X \rightarrow A$ or $X \rightarrow A^\vee$ that maps p to an L -point q not in Γ_0 or not in $\varphi(\Gamma_0)$, respectively. In the former case, we are done. In the latter case, the dual isogeny $\varphi^\vee: A^\vee \rightarrow A$ maps q to $\varphi^\vee(q) \in A(L)$ not lying in Γ_0 , which completes the proof. \square

Proposition 3.7. *Let A be an abelian variety of dimension g over a field k of characteristic zero. Then there exists an extension L/k of degree bounded by a constant d_g as given below such that $A(L)$ contains a non-torsion point:*

- if $g = 1$, we can let $d_g = 2$ when k is a number field and $d_g = 18$ in general.
- if $g \geq 2$, we can let $d_g = 6^{8g} \cdot (8g)!$.

In particular, $A(L)$ is dense in A_L provided that A is geometrically simple.

Proof. The cases $g = 1$ and $g \geq 2$ follow respectively from Theorem 3.2 and Lemma 3.6 by taking $\Gamma = \{0\}$. If A is geometrically simple, then Faltings' theorem on subvarieties of abelian varieties (see [Maz00, Theorem 3.1]) says that the Zariski closure of the subgroup generated by p in A_L coincides with A_L . Hence $A(L)$ is dense in A_L . \square

3.2.2 Existence of a nondegenerate point

Definition 3.8. For an abelian variety A over a field k , we say a rational point $p \in A(k)$ is *nondegenerate* if the subgroup generated by p is Zariski dense in A .

Lemma 3.9. *Let A and A' be abelian varieties over a field k of characteristic zero and let $g' := \dim(A')$. Suppose that A contains a nondegenerate point $p \in A(k)$. Then there exists an extension L/k of degree bounded by $6^{8g'} \cdot (8g)!$ together with a point $p' \in A'(L)$ such that the Zariski closure*

$$B := \overline{\mathbb{Z}(p, p')} \subset (A \times A')_L$$

is an abelian subvariety with $\dim(B) > \dim(A)$.

Proof. The group of homomorphisms $\text{Hom}(A, A')$ is finitely generated as a module over \mathbb{Z} , so the image of p under $\text{Hom}(A, A')$ forms a finitely generated subgroup

$$\Gamma := \text{Hom}(A, A')(p) \subset A'(\bar{k}).$$

When $g' \geq 2$ (resp. $g' = 1$), Lemma 3.6 (resp. Theorem 3.2) implies that there exists an extension L/k of degree bounded by $6^{8g'} \cdot (8g)!$ (resp. at most 18) such that $A'(L)$ contains a point p' not in the saturation of Γ . In any case, it is sufficient to take $6^{8g'} \cdot (8g)!$ as the bound. Let $q := (p, p') \in (A \times A')(L)$ and denote by $B \subset (A \times A')_L$ the abelian subvariety obtained as the Zariski closure of $\mathbb{Z}q$.

Let us prove that $\dim(B) > \dim(A)$ by adapting part of the proof of [HT00, Lemma 3.3]. Assume, to the contrary, that $\dim(B) = \dim(A)$. In this case, the left projection

$$\pi: A \times A' \longrightarrow A$$

restricts to an isogeny $B \longrightarrow A$ over L , so we can regard B as an element in the group of homomorphisms up to isogeny:

$$\beta \in \text{Hom}^0(A, A') := \text{Hom}(A, A') \otimes \mathbb{Q}.$$

In particular, there exists a nonzero integer d such that $(d\beta)(p) = dp'$. This implies that p' lives in the saturation of Γ , contradiction. This proves that $\dim(B) > \dim(A)$. \square

Theorem 3.10. *Let A be an abelian variety of dimension g over a field k of characteristic zero. Then there exists a finite extension L/k of degree bounded by the constant*

$$6^{4g(g+1)} \prod_{r=1}^g (8r)!$$

such that $A(L)$ contains a nondegenerate point.

Proof. By Proposition 3.7, there exists an extension L_1/k of degree at most $6^{8g} \cdot (8g)!$ such that there exists a non-torsion point $p_1 \in A(L_1)$. The Zariski closure of $\mathbb{Z}p_1$ in A_{L_1} is an abelian subvariety A_1 of dimension g_1 by Faltings' theorem. If $g_1 = g$, then p_1 is a

nondegenerate point. If $g_1 < g$, then the quotient $A'_1 := A_{L_1}/A_1$ is an abelian variety of dimension $g - g_1 \geq 1$ and there is an isogeny $A_{L_1} \sim_{L_1} A_1 \times A'_1$. A nondegenerate point can then be found using the inductive process below:

Let $i \geq 1$. Suppose that there exist abelian varieties A_i and A'_i over an extension L_i/k , where A_i contains a nondegenerate point $p_i \in A_i(L_i)$ and $g_i := \dim(A_i) < g$, such that there is an isogeny

$$A_{L_i} \sim_{L_i} A_i \times A'_i. \quad (3.4)$$

By Lemma 3.9, there exists an extension L_{i+1}/L_i with

$$[L_{i+1} : L_i] \leq 6^{8(g-g_i)} \cdot (8(g-g_i))!$$

and a point $p_{i+1} \in (A_i \times A'_i)(L_{i+1})$ such that the Zariski closure of $\mathbb{Z}p_{i+1}$ is an abelian subvariety $A_{i+1} \subset (A_i \times A'_i)_{L_{i+1}}$ of dimension $g_{i+1} > g_i$. If $g_{i+1} = g$, then p_{i+1} induces a nondegenerate point on $A_{L_{i+1}}$ via the isogeny (3.4). If $g_{i+1} < g$, we define

$$A'_{i+1} := (A_i \times A'_i)_{L_{i+1}}/A_{i+1}$$

and repeat the same argument in this paragraph with i replaced by $i + 1$.

As g is fixed, the above process ends up in an abelian variety A_n defined over L_n/L , a nondegenerate point $p_n \in A_n$, and an isogeny $A_{L_n} \sim_{L_n} A_n$ such that p_n induces a nondegenerate point on A_{L_n} . Let $L_0 := k$ and $g_0 := 0$. Using the inequalities $g \geq g_{i+1} > g_i$ for $0 \leq i \leq n-1$, we estimate the degree of extension by

$$\begin{aligned} [L_n : k] &= \prod_{i=0}^{n-1} [L_{i+1} : L_i] \leq \prod_{i=0}^{n-1} 6^{8(g-g_i)} \cdot (8(g-g_i))! \\ &\leq \prod_{i=0}^g 6^{8(g-i)} \cdot (8(g-i))! = 6^{4g(g+1)} \prod_{r=0}^g (8r)! = 6^{4g(g+1)} \prod_{r=1}^g (8r)! \end{aligned}$$

This finishes the proof. \square

Corollary 3.11. *The collection of abelian varieties of a fixed dimension over fields of characteristic zero satisfies uniform potential density.*

Proof. By definition, the orbit of a nondegenerate point is Zariski dense, so the statement follows immediately from Theorem 3.10. \square

3.3 Algebraic groups and their torsors

Unlike torsors of abelian varieties (see Proposition 3.1), we will show that uniform potential density holds for torsors of linear algebraic groups of a fixed dimension over infinite perfect fields. Based on this and the uniform potential density for abelian varieties, we will prove that uniform potential density holds for algebraic groups of a fixed dimension over fields of characteristic zero. In this section, k will denote an infinite perfect field.

3.3.1 Preliminaries on semisimple groups

Let us start by gathering necessary background materials and setting up some notations. Our main reference is [Mil17]. For a connected linear algebraic group G over a field k , its *radical* $R(G)$ is the maximal connected solvable normal subgroup variety. The group G is *semisimple* if $R(G_{\bar{k}})$ is trivial, and is further called *almost simple* if G is noncommutative and every proper normal subgroup is finite. We say that G is *geometrically almost simple* if it is almost simple and remains so over \bar{k} .

Theorem 3.12 ([Mil17, Theorem 21.51]). *A semisimple algebraic group G has only finitely many almost simple normal subgroup varieties G_1, \dots, G_m and the morphism*

$$\begin{array}{ccc} G_1 \times \cdots \times G_m & \longrightarrow & G \\ (g_1, \dots, g_m) & \longmapsto & g_1 \cdots g_m \end{array}$$

is surjective with finite kernel. Moreover, each connected normal algebraic subgroup $H \subset G$ is a product of those G_i 's that H contains, and is centralized by those G_i 's not inside H .

A semisimple group G over k is *split* if there exists a maximal torus $T \subset G$ isomorphic to a product of copies of \mathbb{G}_m over k . By [Tit92, Proposition A1], a geometrically almost simple group G becomes split over an extension L/k of degree dividing an integer $\delta(G)$ depending only on the type of G . Let $v(n)$ denote the 2-adic valuation of an integer n and assume that G is not of type E_8 . Then $\delta(G)$ is given explicitly as

$$\frac{\delta(G)}{\delta(G)} \left| \begin{array}{cccccccccc} A_n & B_n & C_n & D_4 & D_{n \geq 5} & G_2 & F_4 & E_6 & E_7 \\ \hline 2(n+1) & 2^n & 2^{v(n)+1} & 3 \cdot 2^6 & 2^{n+v(n)} & 2 & 6 & 2^2 \cdot 3^4 & 2^5 \cdot 3 \end{array} \right.$$

For G of type E_8 , Totaro [Tot04, Theorem 0.1] improved the result by Tits to

$$\delta(G) = 2^6 \cdot 3^2 \cdot 5.$$

In particular, there exists an increasing function on positive integers

$$\bar{\delta}: \mathbb{N} \longrightarrow \mathbb{N} \quad \text{such that} \quad \delta(G) \leq \bar{\delta}(\dim(G)) \tag{3.5}$$

for every geometrically almost simple group G .

An *inner k -form* of G is an algebraic group G' over k together with an isomorphism $f': G_{\bar{k}} \rightarrow G'_{\bar{k}}$ such that, for every $\sigma \in \text{Gal}(\bar{k}/k)$, the automorphism

$$a_\sigma := f'^{-1} \circ (\sigma f'): G \longrightarrow G, \quad \text{where} \quad \sigma f' := \sigma \circ f' \circ \sigma^{-1}$$

is inner. Two inner k -forms (G', f') and (G'', f'') are isomorphic if there exists an isomorphism $\varphi: G' \rightarrow G''$ over k such that the following diagram commutes:

$$\begin{array}{ccc} G_{\bar{k}} & & \\ f' \downarrow & \searrow f'' & \\ G'_{\bar{k}} & \xrightarrow{\varphi_{\bar{k}}} & G''_{\bar{k}} \end{array}$$

Let $G^{\text{ad}} := G/Z(G)$ where $Z(G)$ is the center of G . When G is semisimple and split, the isomorphism classes of inner k -forms of G are classified by $H^1(k, G^{\text{ad}})$ [Mil17, §24.7]. Moreover, the split ones belong to the distinguished class $[G^{\text{ad}}]$ [Mil17, Corollary 23.54]. Note that, if G is geometrically almost simple, then its inner forms are geometrically almost simple as well.

Let G be semisimple and split as before. According to [CGP15, Corollary A.4.11], there exists a universal covering

$$\beta: \tilde{G} \longrightarrow G$$

where \tilde{G} is a simply connected semisimple group and β is a *central isogeny*, that is, a finite surjective morphism with kernel contained in $Z(\tilde{G})$. This induces a commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & Z(\tilde{G}) & \longrightarrow & \tilde{G} & \longrightarrow & \tilde{G}^{\text{ad}} \longrightarrow 1 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 1 & \longrightarrow & Z(G) & \longrightarrow & G & \longrightarrow & G^{\text{ad}} \longrightarrow 1. \end{array}$$

The map γ is an isomorphism by [BT72, Proposition 2.26]. This fact, together with the surjectivity of β , implies that α is surjective via the snake lemma. Furthermore, we have $\ker(\alpha) \cong \ker(\beta) \cong \pi_1(G)$ since β is central. Therefore,

$$Z(G) \cong Z(\tilde{G})/\pi_1(G). \quad (3.6)$$

Now assume that G is almost simple and split. Then \tilde{G} is almost simple, and $Z(\tilde{G})$ is determined by its type as shown in the table [Mil17, §24-c]:

	A_n	B_n	C_n	D_{2m}	D_{2m+1}	E_6	E_7	E_8, F_4, G_2	
$Z(\tilde{G})$	μ_{n+1}	μ_2	μ_2	$\mu_2 \times \mu_2$	μ_4	μ_3	μ_2	e	(3.7)

where μ_n is the n -th root of unity and e is the identity element. As a consequence, $Z(G)$ is the quotient of one of the above groups, so its size is bounded by a constant depending only on the type of G . We conclude from (3.6) and (3.7) that, for every split almost simple group G , there is an inequality

$$|Z(G)| \leq \begin{cases} n+1 & \text{if } G \text{ is of type } A_n \\ 4 & \text{otherwise.} \end{cases}$$

In particular, there exists an increasing function on positive integers

$$\bar{\zeta}: \mathbb{N} \longrightarrow \mathbb{N} \quad \text{such that} \quad |Z(G)| \leq \bar{\zeta}(\dim(G)) \quad (3.8)$$

for every split almost simple group G .

3.3.2 Torsors under connected linear algebraic groups

We are ready to estimate the degrees of field extensions that make a torsor under a connected linear algebraic group trivial. Let us proceed in a step-by-step manner starting from the case of geometrically almost simple groups. We will need the functions $\bar{\delta}$ and $\bar{\zeta}$ defined in (3.5) and (3.8), respectively.

Lemma 3.13. *Let X be a G -torsor of dimension r where G is a geometrically almost simple algebraic group over a perfect field k . Then there exists an extension L/k of degree bounded by $\bar{\zeta}(r)\bar{\delta}(r)^2$ such that $X_L \cong G_L$.*

Proof. The exact sequence $1 \rightarrow Z(G) \rightarrow G \rightarrow G^{\text{ad}} \rightarrow 1$, when considered over any extension K/k , induces an exact sequence of pointed sets

$$H^1(K, Z(G_K)) \longrightarrow H^1(K, G_K) \longrightarrow H^1(K, G_K^{\text{ad}}).$$

Let $x \in H^1(k, G)$ be the class of X and $y \in H^1(k, G^{\text{ad}})$ be its image under the second map above. By passing to an extension L/k of degree bounded by $\bar{\delta}(r)$, we can assume that G_L is split so that y corresponds to the class of an inner L -form G' of G_L . As G' is also geometrically almost simple of dimension r , there exists an extension L'/L of degree bounded by $\bar{\delta}(r)$ such that $G'_{L'}$ is split. This implies that

$$y = 0 \in H^1(L', G_{L'}^{\text{ad}}) \quad \text{and thus} \quad x \in H^1(L', Z(G_{L'})).$$

Let us take an extension L''/L' with $[L'' : L'] \leq |Z(G_{\bar{k}})| \leq \bar{\zeta}(r)$ such that $\text{Gal}(\bar{L}''/L'')$ acts trivially on $Z(G_{\bar{k}})$ (thus trivially on $Z(G_{L''})$). It follows that $H^1(L'', Z(G_{L''})) = 0$. In particular, $x = 0$ over L'' and we get a desired isomorphism $X_{L''} \cong G_{L''}$. Note that

$$[L'' : k] = [L'' : L'][L' : L][L : k] \leq \bar{\zeta}(r)\bar{\delta}(r)^2$$

so the proof is done. \square

Lemma 3.14. *Let G be a semisimple algebraic group over a perfect field k of dimension $r > 0$. Then there exists an extension L/k of degree bounded by r such that G_L contains a normal subgroup N which is geometrically almost simple with $\dim(N) > 0$.*

Proof. The algebraic group $G_{\bar{k}}$ is still semisimple, so it contains almost simple normal subgroups G_1, \dots, G_m as described in Theorem 3.12, and they are geometrically almost simple since we are over \bar{k} . Because $r = \dim(G) > 0$, there exists G_i where $1 \leq i \leq m$ such that $\dim(G_i) > 0$. Under the action of $\text{Gal}(\bar{k}/k)$, the orbit of G_i is a subset of $\{G_1, \dots, G_m\}$ and thus has cardinality at most $m \leq r$. It follows that there exists an extension L/k of degree bounded by r such that $N := G_i$ is defined over L . \square

Lemma 3.15. *Let X be a G -torsor of dimension r where G is a semisimple algebraic group over a perfect field k . Then there exists an extension L/k of degree bounded by a constant d_r which depends only on and increases with r such that $X_L \cong G_L$.*

Proof. Let us prove the statement by induction on r . Note that the initial case $r = 0$ is trivial. Assume that $r \geq 1$. By Lemma 3.14, after passing to an extension L/k of degree bounded by r , there exists a normal subgroup $N \subset G_L$ that is geometrically almost simple with $\dim(N) > 0$. This induces an exact sequence of pointed sets

$$H^1(L, N) \longrightarrow H^1(L, G_L) \longrightarrow H^1(L, G_L/N).$$

The torsor X represents a class $[X] \in H^1(L, G_L)$. Let $[Y] \in H^1(L, G_L/N)$ be the image of $[X]$, where Y is a G_L/N -torsor. Note that

- G_L/N is semisimple by [Mil17, Corollary 21.52], and
- $\dim(G_L/N) < r$ since $\dim(N) > 0$.

By applying the induction hypothesis on the G_L/N -torsor Y , we obtain an extension L'/L of degree bounded by d_{r-1} such that $[Y_{L'}] = 0 \in H^1(L', G_{L'}/N_{L'})$. This implies that $[X_{L'}]$ is the image of $[Z] \in H^1(L', N_{L'})$ for some $N_{L'}$ -torsor Z .

Let $s := \dim(N)$. Since $N_{L'}$ is geometrically almost simple, Lemma 3.13 implies that there exists an extension L''/L' of degree bounded by $\bar{\zeta}(s)\bar{\delta}(s)^2$ such that

$$[Z_{L''}] = 0 \in H^1(L'', N_{L''}) \quad \text{and thus} \quad [X_{L''}] = 0 \in H^1(L'', G_{L''}).$$

This gives a desired isomorphism $X_{L''} \cong G_{L''}$. Note that

$$[L'' : k] = [L'' : L'][L' : L][L : k] \leq \bar{\zeta}(s)\bar{\delta}(s)^2 \cdot d_{r-1} \cdot r \leq \bar{\zeta}(r)\bar{\delta}(r)^2 \cdot d_{r-1} \cdot r$$

where the last inequality uses $s \leq r$ the fact that $\bar{\delta}$ and $\bar{\zeta}$ are increasing functions. As the last term above depends only on and increases with r , the proof is done. \square

Before entering the general case about torsors under connected linear algebraic groups, we need to discuss the splitting fields of tori. An algebraic group T over a field k is a *torus* if $T_{\bar{k}} \cong \mathbb{G}_m^r$. The integer r is called the *rank* of T . By definition, T is split if and only if $T \cong \mathbb{G}_m^r$ over k .

Lemma 3.16. *Let T be a torus of rank r over a perfect field k . Then there exists an extension L/k of degree bounded by the constant \mathbf{c}_r defined in Definition 2.2 such that T_L is split. In particular, we have $H^1(L, T_L) = \{0\}$.*

Proof. The action of $\text{Gal}(\bar{k}/k)$ on the group of characters

$$X^*(T) := \text{Hom}(T_{\bar{k}}, \mathbb{G}_m) \cong \mathbb{Z}^r$$

induces a homomorphism $\text{Gal}(\bar{k}/k) \rightarrow \text{GL}(r, \mathbb{Z})$, whose kernel is isomorphic to $\text{Gal}(\bar{k}/L)$ for some finite Galois extension L/k . As $\text{Gal}(\bar{k}/L)$ acts on $X^*(T)$ trivially, this implies that T_L is split, that is, $T_L \cong \mathbb{G}_m^r$, due to [Mil17, Theorem 12.23]. Since $\text{Gal}(L/k)$ appears as a finite subgroup of $\text{GL}(r, \mathbb{Z})$, we have $[L : k] = |\text{Gal}(L/k)| \leq \mathbf{c}_r$. The last statement follows from the fact that $H^1(L, \mathbb{G}_m^r) = \{0\}$ (see, e.g., [Mil17, Corollary 3.47]). \square

Proposition 3.17. *Let X be a G -torsor of dimension r where G is a connected linear algebraic group over a perfect field k . Then there exists an extension L/k of degree bounded by the multiplication $d_r \cdot \mathbf{c}_r$ such that $X_L \cong G_L$. Here d_r and \mathbf{c}_r are increasing functions in r given in Lemma 3.15 and Definition 2.2, respectively.*

Proof. Let $U \subset G$ be the unipotent radical. By [San81, Lemma 1.13], there is a canonical isomorphism $H^1(k, G) \cong H^1(k, G/U)$, which reduces the proof to the case when G is reductive.

For a reductive group G , its radical $R \subset G$ is a torus [Mil17, Corollary 17.62]. Let s be the rank of R . By Lemma 3.16, there exists an extension K/k of degree bounded by \mathbf{c}_s such that $H^1(K, R_K) = \{0\}$. This induces an injection

$$0 \longrightarrow H^1(K, G_K) \longrightarrow H^1(K, G_K/R_K).$$

Consider $[X_K] \in H^1(K, G_K)$ as an element in $H^1(K, G_K/R_K)$. Let $t := \dim(G/R)$ and notice that G_K/R_K is semisimple. By Lemma 3.15, there exists an extension L/K of degree bounded by a constant d_t such that $[X_L]$ is trivial in $H^1(L, G_L/R_L)$ and thus is trivial in $H^1(L, G_L)$. It follows that $X_L \cong G_L$. To complete the proof, observe that

$$[L : k] = [L : K][K : k] \leq d_t \cdot \mathbf{c}_s \leq d_r \cdot \mathbf{c}_r$$

where the last inequality follows from the inequalities $s < r$ and $t < r$ as well as the fact that d_r and \mathbf{c}_r increase with r . \square

Corollary 3.18. *Retain the condition of Proposition 3.17 and assume further that k is infinite. Then there exists an extension L/k of degree bounded by $d_r \cdot \mathbf{c}_r$ such that $X(L)$ is dense. In particular, uniform potential density holds for the collection of torsors of connected linear algebraic groups of a fixed dimension over infinite perfect fields.*

Proof. By Proposition 3.17, there exists an extension L/k of degree bounded by $d_r \cdot \mathbf{c}_r$ such that $X_L \cong G_L$. Since k is perfect, G is unirational over k [Bor91, Theorem 18.2 (ii)], which implies that $G(k)$ is dense as k is infinite. This proves that $X(L)$ is dense via the isomorphism $X_L \cong G_L$. \square

Corollary 3.19. *Retain the condition of Proposition 3.17 and assume further that G is quasi-split, that is, contains a Borel subgroup over k . Let r denote the rank of G , that is, the rank of a maximal torus of G . Then there exists an extension L/k of degree bounded by \mathbf{c}_r such that $X_L \cong G_L$.*

Proof. According to [Ste65, Theorem 11.1], there exists a torus $T \subset G$ such that the class $[X] \in H^1(k, G)$ lies in the image of $H^1(k, T)$. Note that $t := \text{rank}(T) \leq r$. By Lemma 3.16, there exists an extension L/k of degree bounded by $\mathbf{c}_t \leq \mathbf{c}_r$ such that $H^1(L, T_L) = \{0\}$, which implies the statement. \square

Remark 3.20. The question about minimal degrees of the field extensions that split torsors under connected linear algebraic groups is also intensively studied. For relevant results and further references in this direction, we refer the reader to [RY01, Tot04].

3.3.3 Connected algebraic groups

Now we have almost everything we need to prove the uniform potential density for connected algebraic groups in characteristic zero.

Lemma 3.21. *Let A be an abelian variety over a field k of characteristic zero with an extension*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} A \longrightarrow 1$$

by a linear algebraic group N over k . Suppose that $A(k)$ contains a nondegenerate point p such that the coset $N_1 := \pi^{-1}(p) \subset G$ contains a dense subset of k -rational points. Then $G(k)$ is dense in G .

Proof. For every $m \in \mathbb{Z}$, we define $N_m := \pi^{-1}(p^m) \subset G$. Note that $N_0 = N$ and that every N_m is an N -torsor under the action

$$N \times N_m \rightarrow N_m : (x, y) \mapsto xy.$$

By hypothesis, N_1 is a trivial N -torsor. This implies that every N_m is trivial since one can produce a k -rational point on N_m via the morphisms

- $N_1^m \rightarrow N_m : x \mapsto x^m$ if $m > 0$,
- $N_{-m} \rightarrow N_m : x \mapsto x^{-1}$ if $m < 0$.

It follows that $N_m(k)$ is dense in N_m for all $m \in \mathbb{Z}$. As a result, we obtain a Zariski dense subset

$$\bigcup_{m \in \mathbb{Z}} N_m(k) \subset G(k)$$

and hence $G(k)$ is dense in G . □

Theorem 3.22. *The collection of connected algebraic groups of a fixed dimension over fields of characteristic zero satisfies uniform potential density.*

Proof. Let G be a connected algebraic group over a field k of characteristic zero. By the Barsotti–Chevalley–Rosenlicht theorem ([Bar55, Che60, Ros56]; see also [Con02, Theorem 1.1]), there is a short exact sequence of algebraic k -groups

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} A \longrightarrow 1$$

where N is a linear closed subgroup of G and A is an abelian variety.

Let $g := \dim(A)$ and $r := \dim(G)$. Notice that $g \leq r$. By Theorem 3.10, there exists an extension L/k of degree bounded by

$$6^{4g(g+1)} \prod_{i=1}^g (8i)! \leq 6^{4r(r+1)} \prod_{i=1}^r (8i)!$$

such that $A(L)$ contains a nondegenerate point. On the other hand, N is unirational over k [Bor91, Theorem 18.2 (ii)], which implies that $N(k)$ is dense in N as k is infinite in our case. Note that the coset $N_1 := \pi^{-1}(p)$ is an N -torsor under the action

$$N \times N_1 \rightarrow N_1 : (x, y) \mapsto xy.$$

Let $n := \dim(N)$. By Corollary 3.18, there exists an extension L'/L of degree bounded by $d_n \cdot \mathbf{c}_n$ such that $N_1(L')$ is dense in $N_1(L)$. (See Lemma 3.15 and Definition 2.2 for the definition of d_r and \mathbf{c}_r .)

The fact that $N_1(L')$ is dense in $N_1(L)$, together with the existence of a nondegenerate point in $A(L)$ (and thus in $A(L')$), implies that $G(L')$ is dense in G by Lemma 3.21. To complete the proof, notice that $d_n \cdot \mathbf{c}_n \leq d_r \cdot \mathbf{c}_r$ since d_r and \mathbf{c}_r are increasing in r . Therefore,

$$[L' : k] = [L' : L][L : k] \leq d_r \cdot \mathbf{c}_r \cdot 6^{4r(r+1)} \prod_{i=1}^r (8i)!$$

where the last term depends only on $r = \dim(G)$. \square

4 Uniform potential density for elliptic K3 surfaces

In this section, we prove that uniform potential density holds for the collection of elliptic K3 surfaces over number fields. Throughout §4.1, the ground field k is assumed to be perfect, or arbitrary with $\text{char}(k) > 5$. In the remaining part of the section, we will specialize to number fields unless otherwise noted.

4.1 Picard groups and automorphisms

Let X be an elliptic K3 surface over k and let k^s denote the separable closure of k . We want to find finite extensions L/k where

- all the elements in $\text{Pic}(X_{k^s})$ descend to $\text{Pic}(X_L)$, or
- a chosen element in $\text{Aut}(X_{k^s})$ is defined.

In each case, we will show that the minimal degree of such extensions L/k is bounded by a constant independent of X . These results will be used to prove the uniform potential density respectively in the cases $\rho(X_{k^s}) \leq 19$ and $\rho(X_{k^s}) = 20$.

4.1.1 Defining fields of Picard groups

Let X be an elliptic K3 surface over a field k . For every separable extension L/k , there are natural injections

$$\text{Pic}(X_L) \hookrightarrow \text{Pic}(X_{k^s})^{\text{Gal}(k^s/L)} \hookrightarrow \text{Pic}(X_{k^s}). \quad (4.1)$$

Our goal is to find a separable extension L/k such that the two injections become isomorphisms with the degree $[L : k]$ bounded. Let us discuss the injection on the left first.

In general, for every proper and geometrically integral variety X over a field k , there is an exact sequence [Poo17, Corollary 6.7.8]:

$$0 \longrightarrow \text{Pic}(X) \longrightarrow \text{Pic}(X_{k^s})^{\text{Gal}(k^s/k)} \longrightarrow \text{Br}(k) \longrightarrow \text{Br}(X)$$

If $X(k) \neq \emptyset$, then the morphism $\text{Spec}(k) \rightarrow X$ induces a section $\text{Br}(X) \rightarrow \text{Br}(k)$. Under this condition, the last map of the sequence is injective, which forces the second map to be an isomorphism

$$\text{Pic}(X) \xrightarrow{\sim} \text{Pic}(X_{k^s})^{\text{Gal}(k^s/k)}.$$

Therefore, to make the first injection in (4.1) an isomorphism, it is sufficient to find a separable extension L/k such that $X(L) \neq \emptyset$.

Let us analyze this property for a general elliptic surface. Recall that the Euler–Poincaré characteristic $\chi(Z)$ is defined by

$$\chi(Z) = \sum_i (-1)^i \dim H_{\text{et}}^i(Z_{\bar{k}}, \mathbb{Q}_\ell), \quad \text{where } \ell \neq \text{char}(k).$$

For an elliptic surface $\pi: X \rightarrow C$, we have [CD89, Proposition 5.1.6]:

$$\chi(X) = \sum_{b \in C(\bar{k})} \chi(X_b). \quad (4.2)$$

Here the sum is finite as $\chi(X_b) = 0$ if X_b is smooth. Given a fiber X_b over $b \in C(k^s)$, we denote by $\#X_b$ the number of its geometrically irreducible components (ignoring the multiplicities). For a singular X_b , we have $\chi(X_b) = \#X_b$ or $\chi(X_b) = \#X_b + 1$ depending on its type. The assumption that k is perfect or arbitrary with $\text{char } k > 5$ implies that the singular fibers are all of classical Kodaira types. (See [CD89, Proposition 3.1.1] for the perfect case and [LLR04, Appendix A] for the other case.)

Lemma 4.1. *Let $\pi: X \rightarrow C$ be an elliptic surface over k and let $X_b \subset X$ be a singular fiber over $b \in C(k^s)$ with minimal possible $\chi(X_b)$. Then, for any reduced and geometrically irreducible component $D \subset X_b$, there exists a separable extension L/k of degree at most $2\chi(X)$ such that D is birational to \mathbb{P}_L^1 . In particular, we have $X(L) \supset D(L) \neq \emptyset$.*

Proof. Consider the set

$$\Sigma^s := \{b \in C(k^s) \mid X_b \text{ is singular}\} \neq \emptyset.$$

Then there exists a separable extension L_1/k of degree at most $|\Sigma^s|$ such that the point $b \in \Sigma^s$, and thus X_b , is defined over L_1 . According to Kodaira’s table, the component D appears in X_b either as a reduced component or with higher multiplicity divisible by only 2, 3, or 5. Because $\text{char}(k) > 5$, this implies that D is defined over a separable extension L_2/L_1 of degree at most $\#X_b \leq \chi(X_b)$. The normalization of D is a smooth conic, which is isomorphic to \mathbb{P}_L^1 over a separable extension L/L_2 of degree at most 2. In particular, D_L is birational to \mathbb{P}_L^1 and thus $X(L) \supset D(L) \neq \emptyset$. About the degree of L/k , we have

$$[L : k] = [L : L_2][L_2 : L_1][L_1 : k] \leq 2\chi(X_b)|\Sigma^s|.$$

Using the minimality of $\chi(X_b)$ and (4.2), we obtain

$$2\chi(X_b)|\Sigma^s| \leq 2 \sum_{b \in \Sigma^s} \chi(X_b) \leq 2\chi(X).$$

Combine this inequality with the one above, we conclude that $[L : k] \leq 2\chi(X)$. \square

Lemma 4.2. *Every elliptic K3 surface X over k has a singular fiber over k^s .*

Proof. In the case that k is perfect, we have $k^s = \bar{k}$. Suppose, to the contrary, that $X_{\bar{k}}$ has no singular fiber. Then $\chi(X) = 0$ by (4.2), which contradicts to the fact that $\chi(X) = 24$ for every K3 surface X . Therefore, X has a singular fiber over $k^s = \bar{k}$.

Now assume that k is arbitrary with $\text{char}(k) > 5$. When X has a section, it admits a Weierstrass model $W \rightarrow \mathbb{P}^1$ (see, e.g., [Huy16, §11.2]):

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

where $g_2 \in H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(8))$ and $g_3 \in H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(12))$. Its discriminant is given by

$$\Delta = g_2^3 - 27g_3^2 \in H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(24)).$$

If W has no singular fiber over k^s , then $\text{char}(k)$ divides $\deg(\Delta) = 24$, which contradicts to the hypothesis that $\text{char}(k) > 5$. Therefore, W has a singular fiber over k^s . This implies that X has a singular fiber over k^s as well.

In general, we can associate X with its Jacobian fibration $J(X)$, which is an elliptic K3 surface with a section. There exists a dominant rational map $f: X \dashrightarrow J(X)$ preserving the fibrations, which acts by mapping a smooth fiber to its Jacobian. (See §4.2.1 for a brief introduction on $J(X)$.) We have proved that $J(X)$ has a singular fiber over k^s , so X has a singular fiber over k^s as f maps a singular fiber to a singular fiber. \square

Corollary 4.3. *Let X be an elliptic K3 surface over k . Then there exists a separable extension L/k of degree at most 48 such that, for every separable extension L'/L , the natural inclusion*

$$\text{Pic}(X_{L'}) \hookrightarrow \text{Pic}(X_{k^s})^{\text{Gal}(k^s/L')}$$

is an isomorphism

Proof. The surface X has a singular fiber over k^s by Lemma 4.2, so Lemma 4.1 guarantees the existence of a separable extension L/k of degree at most $2\chi(X) = 2 \cdot 24 = 48$ such that $X(L) \neq \emptyset$. Hence $X(L') \neq \emptyset$ for every separable extension L'/L , which implies the conclusion. \square

Recall that by Theorem 2.1, the group $\text{GL}(n, \mathbb{Z})$ contains, up to isomorphism, only finitely many finite subgroups and \mathbf{c}_n denotes the largest possible cardinality of such subgroup. Now let us study the injection on the right in (4.1).

General versions of the following lemma for K3 surfaces have appeared in the literature under the assumption of the existence of a rational point (e.g. [Huy16, Lemma 17.2.6]). The version we present here is specific to elliptic K3 surfaces without this assumption.

Lemma 4.4. *Let X be an elliptic K3 surface over k and denote $\rho := \rho(X_{k^s})$. Then there exists a separable extension L/k of degree at most $48\mathbf{c}_\rho$ such that there is a natural isomorphism*

$$\text{Pic}(X_L) \xrightarrow{\sim} \text{Pic}(X_{k^s}).$$

Proof. By Corollary 4.3, there exists a separable extension L_1/k of degree at most 48 such that, for every separable extension L'/L_1 , there is a natural isomorphism

$$\mathrm{Pic}(X_{L'}) \xrightarrow{\sim} \mathrm{Pic}(X_{k^s})^{\mathrm{Gal}(k^s/L')}. \quad (4.3)$$

The Galois action on $\mathrm{Pic}(X_{k^s})$ induces a group homomorphism

$$\sigma : \mathrm{Gal}(k^s/L_1) \longrightarrow \mathrm{GL}(\rho, \mathbb{Z}).$$

Since $\mathrm{Pic}(X_{k^s})$ is finitely generated, the kernel is finite index in $\mathrm{Gal}(k^s/k)$, corresponding to a finite extension L/L_1 . Hence, $\mathrm{Gal}(k^s/L) = \ker(\sigma)$. This identifies the finite group $\mathrm{Gal}(L/L_1)$ as a subgroup of $\mathrm{GL}(\rho, \mathbb{Z})$, and so $[L : L_1] = |\mathrm{Gal}(L/L_1)|$ is bounded by \mathbf{c}_ρ . We conclude that there exists a Galois extension L/L_1 of degree at most \mathbf{c}_ρ such that

$$\mathrm{Pic}(X_{k^s})^{\mathrm{Gal}(k^s/L)} = \mathrm{Pic}(X_{k^s}). \quad (4.4)$$

The desired isomorphism follows immediately from (4.3) and (4.4). Moreover, we have $[L : k] = [L : L_1] \cdot [L_1 : k] \leq \mathbf{c}_\rho \cdot 48$. \square

4.1.2 Defining fields of automorphisms on K3 surfaces

Let us introduce some notations first. For a K3 surface X over k , the group $\mathrm{Aut}(X_{k^s})$ acts on $\mathrm{Pic}(X_{k^s})$ by pulling back line bundles,

$$\mathrm{Aut}(X_{k^s}) \longrightarrow \mathrm{O}(\mathrm{Pic}(X_{k^s})) : f \longmapsto f^*.$$

We will also consider the action of $\mathrm{Gal}(k^s/k)$ on $\mathrm{Aut}(X_{k^s})$ by

$$\begin{aligned} \mathrm{Gal}(k^s/k) \times \mathrm{Aut}(X_{k^s}) &\longrightarrow \mathrm{Aut}(X_{k^s}) \\ (\sigma, f) &\longmapsto f^\sigma := \sigma^{-1} f \sigma. \end{aligned}$$

For every separable extension L/k , we have

$$\mathrm{Aut}(X_L) = \mathrm{Aut}(X_{k^s})^{\mathrm{Gal}(k^s/L)}$$

under the above action.

Proposition 4.5. *Let X be a K3 surface over k that satisfies $\mathrm{Pic}(X) = \mathrm{Pic}(X_{k^s})$. Then, for every $f \in \mathrm{Aut}(X_{k^s})$, there exists an integer $n > 0$ such that $f^n \in \mathrm{Aut}(X)$.*

Proof. By hypothesis, $\mathrm{Gal}(k^s/k)$ acts on $\mathrm{Pic}(X_{k^s})$ trivially. Let us fix some $f \in \mathrm{Aut}(X_{k^s})$ and $\sigma \in \mathrm{Gal}(k^s/k)$. Then, for every $\mathcal{L} \in \mathrm{Pic}(X_{k^s})$, we have

$$(f^\sigma)^* \mathcal{L} = (\sigma^{-1} f \sigma)^* \mathcal{L} = \sigma f^* (\sigma^{-1})^* \mathcal{L} = \sigma(f^* \mathcal{L}) = f^* \mathcal{L}$$

where the hypothesis on the Galois action is applied to the last two equalities. Hence

$$(f^\sigma f^{-1})^* \mathcal{L} = (f^{-1})^* (f^\sigma)^* \mathcal{L} = (f^*)^{-1} (f^\sigma)^* \mathcal{L} = \mathcal{L}.$$

This implies that $f^\sigma f^{-1} \in \ker(\text{Aut}(X_{k^s}) \rightarrow \text{O}(\text{Pic}(X_{k^s})))$.

Applying the above argument to f^ℓ where $\ell \in \mathbb{Z}$, we conclude that

$$\{(f^\sigma)^\ell f^{-\ell} \mid \ell \in \mathbb{Z}\} \subset \ker(\text{Aut}(X_{k^s}) \rightarrow \text{O}(\text{Pic}(X_{k^s}))).$$

The kernel on the right is finite by [Huy16, Proposition 5.3.3], so the set on the left is finite as well. In particular, there exist distinct integers i and j such that

$$(f^\sigma)^i f^{-i} = (f^\sigma)^j f^{-j}, \text{ or equivalently, } f^{i-j} = (f^\sigma)^{i-j} = (f^{i-j})^\sigma.$$

In other words, f^m , where $m := |i - j| > 0$, is fixed by $\sigma \in \text{Gal}(k^s/k)$.

The integer m may depend on σ . However, as f is defined over some finite separable extension over L , it is fixed by some finite index subgroup $H \subset \text{Gal}(k^s/k)$. Let $\sigma_1, \dots, \sigma_r \in \text{Gal}(k^s/k)$ be representatives for the cosets. Then we can associate each σ_i an integer m_i as above so that f^{m_i} is fixed by σ_i . Define $n := \prod_{i=1}^r m_i$. Then f^n is fixed by each σ_i and thus is fixed by $\text{Gal}(k^s/k)$, so $f^n \in \text{Aut}(X)$. This finishes the proof. \square

4.2 Jacobian fibrations and rational multisections

A main ingredient in Bogomolov and Tschinkel's [BT00] proof of potential density is about the existence of a non-torsion rational multisection. In this section, we show that one can find such a multisection over a finite extension of bounded degree.

4.2.1 Jacobian fibrations of elliptic K3 surfaces

Let us start with a brief review on the Jacobian fibrations of elliptic K3 surfaces. For the general foundations on torsors and their classifying spaces, we refer the reader to [Poo17, Chapter 6] and [Mil80, Chapter III]. We also refer the reader to [Huy16, §11.4 and §11.5] for more details of the following materials treated over algebraically closed fields.

Let $\pi: X \rightarrow \mathbb{P}^1$ be an elliptic K3 surface over a perfect field k and let η denote the generic point of the base \mathbb{P}^1 . The generic fiber X_η is a genus one curve over the function field $K := k(\mathbb{P}^1)$, so we can talk about its Jacobian

$$J(X_\eta) := \text{Pic}_{X_\eta/K}^0.$$

The Jacobian $J(X_\eta)$ has a natural structure of an elliptic curve as it contains the K -rational point $[\mathcal{O}_{X_\eta}]$. On the other hand, it is also a surface over k and thus admits a minimal model $J(X)$. The surface $J(X)$, called the *Jacobian fibration* of X , is an elliptic K3 surface equipped with a section from the point $[\mathcal{O}_{X_\eta}]$. In the following, an elliptic K3 surface with a section will be called a Jacobian fibration.

Given a Jacobian fibration $\pi: J \rightarrow \mathbb{P}^1$, its étale local sections form a sheaf \mathcal{J} of abelian groups on \mathbb{P}^1 . There is a natural bijection

$$H^1(\mathbb{P}^1, \mathcal{J}) \longleftrightarrow \{\text{Elliptic K3 surfaces } X \rightarrow \mathbb{P}^1 \text{ with } J(X) \cong J\} / \sim$$

where $X \sim X'$ if and only if they are isomorphic as elliptic fibrations. It is well known that the group $H^1(\mathbb{P}^1, \mathcal{J})$ is torsion. Hence, to every elliptic K3 surface X with $J(X) \cong J$, we can assign a positive integer $\text{ind}(X)$ called the *index* of X , defined as the order of its class $[X]$ in $H^1(\mathbb{P}^1, \mathcal{J})$. Equivalently, the index of X is the index of the image of the group homomorphism

$$\begin{array}{ccc} \text{Pic}(X) & \longrightarrow & \mathbb{Z} \\ D \mapsto & \longrightarrow & D \cdot X_b \end{array}$$

where X_b is the fiber over a general $b \in \mathbb{P}^1(\bar{k})$.

Given $[X], [Y] \in H^1(\mathbb{P}^1, \mathcal{J})$ such that $[X] = n[Y]$ for some positive integer n , there exists a commutative diagram of dominant k -rational maps of elliptic fibrations:

$$\begin{array}{ccc} Y & \dashrightarrow & X \\ & \searrow & \downarrow \\ & & J. \end{array} \tag{4.5}$$

Let ℓ and m be the indices of $[X]$ and $[Y]$, respectively. Then $\ell = nm$, and over a point $b \in \mathbb{P}^1(k)$ where the fibers are smooth, these maps act as

$$\begin{array}{ccc} Y_b \cong \text{Pic}_{Y_b/k}^1 & \dashrightarrow & X_b \cong \text{Pic}_{Y_b/k}^n \\ & \searrow & \downarrow \\ & & J_b \cong \text{Pic}_{Y_b/k}^\ell. \end{array}$$

For example, the downward arrow on the right maps \mathcal{L} to $\mathcal{L}^{\otimes m}$.

The following lemma is well known to experts. We include a proof from the MathOverflow post [BS16] by Lior Bary-Soroker based on the *embedding problems* (c.f. [FJ08, Definition 16.4.1]).

Lemma 4.6. *Let k be a Hilbertian field (e.g., the function field of \mathbb{P}^1 over a number field) and M a nonzero finite $\text{Gal}(\bar{k}/k)$ -module. Then, $H^1(k, M)$ is infinite.*

Proof. Let $G_k := \text{Gal}(\bar{k}/k)$ and $U \subset G_k$ be an open subgroup such that the action on M factors through $G := G_k/U$. For each integer $n > 0$, we consider the semidirect product of groups

$$\Gamma_n := M^n \rtimes G$$

where G acts on M^n by $g \cdot (m_1, \dots, m_n) = (gm_1, \dots, gm_n)$. Since the field k is Hilbertian, there exists a surjective homomorphism $\psi: G_k \rightarrow \Gamma_n$ and a commutative diagram

$$\begin{array}{ccc} G_k & \xrightarrow{\psi} & \Gamma_n \\ & \searrow r & \downarrow p \\ & & G \end{array}$$

where $r: G_k \rightarrow G$ is the quotient map and $p: \Gamma_n \rightarrow G$ is the second projection (c.f. [FJ08, Proposition 16.4.5]).

For each $i = 1, \dots, n$, we define

$$\pi_i: \Gamma_n \longrightarrow \Gamma_1 : ((m_1, \dots, m_n), g) \mapsto (m_i, g)$$

and let $\psi_i = \pi_i \circ \psi$. Since M is nontrivial, it contains at least two distinct elements m and m' . For any $i \neq j$, let $\gamma_{ij} \in M^n$ be an element whose i -th entry is m and j -th entry is m' . By the surjectivity of ψ , there exists $g \in G_k$ such that $\psi(g) = (\gamma_{ij}, 0) \in \Gamma_n$. Since $r(g) = p \circ \psi(g) = 0$, it follows that $g \in U$. Notice that $\psi_i(g) = (m, 0) \neq (m', 0) = \psi_j(g)$. This shows that, for any $i \neq j$, there exists $u \in U$ such that $\psi_i(u) \neq \psi_j(u)$.

For each $1 \leq i \leq n$, define $c_i: G_K \rightarrow M$ to be the composition

$$c_i: G_k \xrightarrow{\psi_i} \Gamma_1 = M \rtimes G \xrightarrow{q} M.$$

where q is the projection to M . We claim that each c_i is a 1-cocycle, that is, $c_i(gh) = c_i(g) + gc_i(h)$ for any $g, h \in G_k$. For the sake of simplicity, we denote the images of g and h under $r: G_k \rightarrow G$ as \bar{g} and \bar{h} , respectively. Since ψ_i is a homomorphism,

$$q(\psi_i(g)\psi_i(h)) = q((c_i(g), \bar{g})(c_i(h), \bar{h})) = q(c_i(g) + \bar{g}c_i(h), \bar{g}\bar{h}) = c_i(g) + \bar{g}c_i(h)$$

which verifies the claim. Next we show that c_i and c_j are distinct modulo 1-coboundaries for any $i \neq j$. Recall that there exists $u \in U$ such that $\psi_i(u) \neq \psi_j(u)$. This implies that $c_i(u) \neq c_j(u)$ as $\psi_\ell(u) = (c_\ell(u), 0)$ for all ℓ . Since $d(u) = 0$ every 1-coboundary $d: G_k \rightarrow M$ and $u \in U$, the claim follows. We have shown that each c_i gives a distinct class in $H^1(k, M)$, which shows this group is infinite by letting $n \rightarrow \infty$. \square

Lemma 4.7. *Let $\pi: J \rightarrow \mathbb{P}^1$ be a Jacobian fibration over a number field k and let \mathcal{J} be the associated sheaf on \mathbb{P}^1 . Then $H^1(\mathbb{P}^1, \mathcal{J})[n]$ contains infinitely many elements for any $n > 1$.*

Proof. Let η denote the generic point of \mathbb{P}^1 . Let $K/\bar{k}(\eta)$ be a finite Galois extension such that $J_\eta(K)[n] = J_\eta(\bar{K})[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$ is the full n -torsion subgroup. Let $C_{\bar{k}} \rightarrow \mathbb{P}_{\bar{k}}^1$ be the Galois cover of smooth projective curves over \bar{k} corresponding to $K/\bar{k}(\eta)$. Denote by G the Galois group $\text{Gal}(K/k(\eta))$. The Hochschild–Serre spectral sequence

$$E_2^{p,q} = H^p(G, H^q(C_{\bar{k}}, \mathcal{J})) \implies H^{p+q}(\mathbb{P}^1, \mathcal{J})$$

and the isomorphism $H^0(C_{\bar{k}}, \mathcal{J}) \simeq J_\eta(K)$ give an injection $H^1(G, J_\eta(K)) \hookrightarrow H^1(\mathbb{P}^1, \mathcal{J})$, which restricts to an injection

$$H^1(G, J_\eta(K))[n] \hookrightarrow H^1(\mathbb{P}^1, \mathcal{J})[n]. \quad (4.6)$$

Consider $M := J_\eta(K)$ as a G -module. The Kummer sequence

$$0 \longrightarrow M[n] \longrightarrow M \xrightarrow{\times n} M \longrightarrow 0$$

induces the exact sequence

$$0 \longrightarrow \frac{J_\eta(k(\eta))}{nJ_\eta(k(\eta))} \longrightarrow H^1(G, M[n]) \longrightarrow H^1(G, M)[n] \longrightarrow 0.$$

The quotient $J_\eta(k(\eta))/nJ_\eta(k(\eta))$ is finite by the Mordell–Weil theorem over function fields. By Lemma 4.6, the group $H^1(k(\eta), M[n])$ is infinite. Hence, by enlarging K , we can make $H^1(G, M[n])$ arbitrarily large. (Note that $M[n]$ does not change upon enlarging K .) It follows then that $H^1(G, M)[n]$ can also be made arbitrarily large, and thus $H^1(\mathbb{P}^1, \mathcal{J})[n]$ must be infinite by (4.6). \square

Lemma 4.8. *Let G be an abelian group that contains an element of prime order p . Then, for every $x \in G$ whose order is finite and not divisible by p , there exists $z \in G$ such that $pz = x$ and $p \mid \text{ord}(z)$.*

Proof. Let $d := \text{ord}(x)$. First we show that there exists $\beta \in \mathbb{Z}$ such that

$$\beta d \equiv 1 \pmod{p} \quad \text{and} \quad \beta d \not\equiv 1 \pmod{p^2}. \quad (4.7)$$

There exists β satisfying the first equation since p and d are coprime. If $\beta d \not\equiv 1 \pmod{p^2}$, then we are done. If $\beta d \equiv 1 \pmod{p^2}$, then

$$(\beta + p)d \equiv 1 + pd \not\equiv 1 \pmod{p^2},$$

where the second relation uses the assumption $p \nmid d$. Note that $(\beta + p)d \equiv 1 \pmod{p}$. Therefore, we can replace β by $\beta + p$ to fulfill (4.7).

Let $\alpha \in \mathbb{Z}$ be such that $\alpha p + \beta d = 1$. Note that by (4.7), we have $p \nmid \alpha$. Pick an element $y \in G$ of order p and define $z := \alpha(x + y)$. Then

$$pz = p\alpha(x + y) = p\alpha x = (1 - \beta d)x = x - \beta dx = x.$$

It follows that $\text{ord}(z) \mid pd$. We claim that $\text{ord}(z) \nmid d$. Indeed, if $\text{ord}(z)$ divides d , then

$$0 = dz = d\alpha(x + y) = d\alpha y,$$

which implies that $p \mid d\alpha$ and thus $p \mid \alpha$, contradiction. Therefore, we have $p \mid \text{ord}(z)$. \square

Proposition 4.9. *Let $\pi: J \rightarrow \mathbb{P}^1$ be a Jacobian fibration over a number field k . For every $[X] \in H^1(\mathbb{P}^1, \mathcal{J})$ and every prime $p \nmid \text{ind}(X)$, there exists $[Y] \in H^1(\mathbb{P}^1, \mathcal{J})$ such that $[X] = p[Y]$ and $p \mid \text{ind}(Y)$.*

Proof. By Lemma 4.7, the group $H^1(\mathbb{P}^1, \mathcal{J})[p']$ is infinite for every prime p' . In particular, for every prime p as in the statement, $H^1(\mathbb{P}^1, \mathcal{J})$ contains an element of prime order p . Now apply Lemma 4.8 with $G = H^1(\mathbb{P}^1, \mathcal{J})$ to get the desired Y . \square

4.2.2 Existence of non-torsion rational multisections

Let $\pi: X \rightarrow \mathbb{P}^1$ be an elliptic K3 surface over a perfect field k and let \mathcal{J} be the associated Jacobian sheaf. Following [BT00, Definition 3.7], we say that a multisection $\mathcal{M} \subset X$ is *torsion of order m* or *m -torsion* if m is the smallest positive integer such that for every $b \in \mathbb{P}^1(\bar{k})$ and $p, q \in \mathcal{M} \cap X_b(\bar{k})$, the class $[p] - [q]$ lies in $\mathcal{J}_b[m]$.

We call \mathcal{M} *non-torsion* or an *nt-multisection* if there exists $b \in \mathbb{P}^1(\bar{k})$ such that $[p] - [q] \in \mathcal{J}_b$ is torsion-free for some $p, q \in \mathcal{M} \cap X_b(\bar{k})$. Recall that there exists such a $b \in \mathbb{P}^1(\bar{k})$ if and only if the statement holds for a general point in $\mathbb{P}^1(\bar{k})$ by [BT00, Lemma 3.8].

Lemma 4.10. *Pick any $[X], [Y] \in H^1(\mathbb{P}^1, \mathcal{J})$ that satisfy $[X] = n[Y]$ and let $\varphi: Y \dashrightarrow X$ be the map given in (4.5). Then a multisection $\mathcal{M} \subset Y$ is non-torsion if and only if its image $\varphi(\mathcal{M}) \subset X$ is non-torsion.*

Proof. It is easy to see that \mathcal{M} is torsion implies that $\varphi(\mathcal{M})$ is torsion. Let us assume that \mathcal{M} is non-torsion. Then there exist $b \in \mathbb{P}^1(\bar{k})$ and $p, q \in Y_b(\bar{k})$ such that Y_b is smooth and $[p] - [q] \in \text{Pic}^0(Y_b)$ is non-torsion. Choose p and $\varphi(p)$ as origins for Y_b and X_b , respectively. We can identify $\varphi|_{Y_b}$ as the isogeny $[n]: \mathcal{J}_b \rightarrow \mathcal{J}_b$, where $[n]$ is the multiplication by n . Under this identification, q is non-torsion, and thus $\varphi(q)$ is non-torsion. It follows that $[\varphi(q)] - [\varphi(p)] \in \text{Pic}^0(X_b)$ is non-torsion, so $\varphi(\mathcal{M}) \subset X$ is non-torsion. \square

Given a relatively minimal Jacobian fibration $J \rightarrow \mathbb{P}^1$, we consider the invariant $c(J)$ defined by Hassett [Has03, Corollary 9.5]. Suppose that, with respect to Kodaira's table of singular fibers, J has n_0 fibers of type I_0^* , n_1' fibers of type I_a with $a > 0$, n_1'' fibers of type I_a^* with $a > 0$, n_2 fibers of type II or II*, n_3 fibers of type III or III*, and n_4 fibers of types IV or IV*. Then $c(J)$ is defined by

$$c(J) = \frac{1}{2}n_0 + n_1' + n_1'' + \frac{5}{6}n_2 + \frac{3}{4}n_3 + \frac{2}{3}n_4 - 2. \quad (4.8)$$

Lemma 4.11. *Let X be an elliptic K3 surface over a number field k with associated Jacobian fibration J and Jacobian sheaf \mathcal{J} . Suppose that $c(J) > 0$. Then there exists a prime p and a class $[Y] \in H^1(\mathbb{P}^1, \mathcal{J})$ such that $[X] = p[Y]$ and every rational multisection on Y is non-torsion.*

Proof. By Proposition 4.9, for every prime $p \nmid \text{ind}(X)$, there exists $[Y] \in H^1(\mathbb{P}^1, \mathcal{J})$ such that $[X] = p[Y]$ and $\text{ind}(Y) = pd$ for some $d > 0$. Let $[Y'] = d[Y] \in H^1(\mathbb{P}^1, \mathcal{J})$. Then $\text{ind}(Y') = p$ and we have rational maps between elliptic fibrations:

$$Y \xrightarrow{\varphi} Y' \dashrightarrow J.$$

Let $\mathcal{M} \subset Y$ be a rational multisection and suppose, to the contrary, that it is torsion. Then the multisection $\varphi(\mathcal{M}) \subset Y'$ is torsion by Lemma 4.10. Corollary 3.10 of [BT00] then implies that $\varphi(\mathcal{M})$ admits a surjection onto one of the p -torsion multisections either on Y' or $J - \{\text{zero section}\}$. However, the irreducible components of these p -torsion multisections have positive genus provided that $p \gg 0$ due to $c(J) > 0$ and [Has03, Corollaries 8.3, 9.5, and Theorem 9.9]. Hence $\varphi(\mathcal{M})$, and thus \mathcal{M} , is non-torsion if $p \gg 0$. \square

Lemma 4.12. *Let X be an elliptic K3 surface over a number field k . Then there exists a finite extension L/k of degree at most $48^2 \mathbf{c}_{20}$ such that there is a rational multisection $\mathcal{M} \subset X_L$ defined over L .*

Proof. By hypothesis, the group $\text{Pic}(X)$ contains primitive classes H and E where H is ample and E defines an elliptic fibration. They span a sublattice $\langle H, E \rangle \subset \text{Pic}(X)$ with intersection products

$$\begin{pmatrix} 2a & r \\ r & 0 \end{pmatrix}, \quad \text{where } a > 0 \text{ and } r > 0.$$

Define $L := rH - aE$. Then $L^2 = 0$ and $L \cdot H = ar > 0$, which imply that L is effective by Riemann–Roch. We claim that there exist an elliptic curve E' and (-2) -curves C_1, \dots, C_ℓ over the algebraic closure \bar{k} such that

$$L = m_0 E' + \sum_{i=1}^{\ell} m_i C_i \in \text{Pic}(X_{\bar{k}}), \quad \text{where } m_0, \dots, m_\ell > 0.$$

Indeed, if L is nef, then $L = m_0 E'$ for some elliptic curve E' and positive integer m_0 by [Huy16, Proposition 2.3.10], so the claim holds in this case. If L is not nef, one can follow the procedure in [Huy16, Remark 8.2.13] to find (-2) -curves C_i and positive integers m_i , where $1 \leq i \leq \ell$, such that $L - \sum_{i=1}^{\ell} m_i C_i$ is effective and nef. Using [Huy16, Proposition 2.3.10] again, we conclude that $L - \sum_{i=1}^{\ell} m_i C_i = m_0 E'$ for some elliptic curve E' and $m_0 > 0$, which proves the claim.

Let us denote the fibration defined by E as $\pi_E: X \rightarrow \mathbb{P}^1$ and the fibration defined by E' as $\pi_{E'}: X \rightarrow \mathbb{P}^1$. We claim that π_E admits a rational multisection given by

- (a) one of the (-2) -curves C_i , where $1 \leq i \leq \ell$, or
- (b) a reduced and geometrically irreducible component D of a singular fiber X_b with minimal possible $\chi(X_b)$ in the fibration $\pi_{E'}: X \rightarrow \mathbb{P}^1$.

In the case that $E = E'$, we have

$$\sum_{i=1}^{\ell} m_i (C_i \cdot E) = L \cdot E = (rH - aE) \cdot E = r^2 > 0.$$

Hence π_E admits a multisection as in (a). Suppose that $E \neq E'$ and that C_i is not a multisection of π_E for every i . Then every fiber of $\pi_{E'}$ is as a multisection of π_E since

$$E' \cdot E = \frac{1}{m_0} \left(L - \sum_{i=1}^{\ell} m_i C_i \right) \cdot E = \frac{1}{m_0} L \cdot E = \frac{1}{m_0} (rH - aE) \cdot E = \frac{1}{m_0} \cdot r^2 > 0.$$

In particular, we can find a multisection as in (b) by picking a singular fiber X_b with minimal possible $\chi(X_b)$ and then choosing a reduced and geometrically irreducible component $D \subset X_b$ that appears as a multisection of π_E .

Now let us find the field extensions where the multisections of types (a) and (b) are defined. By Lemma 4.4, there exists an extension L_1/k of degree at most $48\mathbf{c}_p \leq 48\mathbf{c}_{20}$ such that $\text{Pic}(X_{L_1}) \cong \text{Pic}(X_{\bar{k}})$. Note that C_i for $i = 1, \dots, \ell$ are defined over L_1 as they are (-2) -curves. Therefore, the proof is done if we are in case (a). Suppose that we are in case (b). Note that the class E' , and thus the fibration $\pi_{E'}$, is defined over L_1 . By Lemma 4.1, there exists an extension L/L_1 of degree at most $2\chi(X) = 48$ over which D is birational to \mathbb{P}_L^1 . Moreover, $[L : k] = [L : L_1][L_1 : k] = 48^2 \mathbf{c}_{20}$, so the proof is done. \square

Proposition 4.13. *Let X be an elliptic K3 surface over a number field k . Suppose that its associated Jacobian fibration J satisfies $c(J) > 0$. Then there exists an extension L/k of degree at most $48^2 \mathbf{c}_{20}$ and a non-torsion rational multisection $\mathcal{M} \subset X_L$ over L .*

Proof. By Lemma 4.11, there exists $[Y] \in H^1(\mathbb{P}^1, \mathcal{J})$ such that $[X] = p[Y]$ for some prime p and every rational multisection on Y is non-torsion. This fact, together with Lemma 4.12, implies the existence of an extension L/k of degree at most $48^2 \mathbf{c}_{20}$ and a non-torsion rational multisection $\mathcal{M} \subset Y_L$. The image of \mathcal{M} under the map $Y_L \dashrightarrow X_L$ gives a rational multisection on X_L that, by Lemma 4.10, is non-torsion as well. \square

4.3 Proof of uniform potential density

Let us finish the proof of uniform potential density for elliptic K3 surfaces.

Theorem 4.14. *For every elliptic K3 surface $\pi: X \rightarrow \mathbb{P}^1$ over a number field k , there exists an extension L/k of degree at most $4608 \mathbf{c}_{20}$ such that $X(L)$ is dense in Zariski topology.*

The Jacobian fibration $J = J(X)$ determines an invariant $c(J)$ that was defined by Hassett [Has03, Corollary 9.5]. (See (4.8) for the definition.) We proceed the proof with respect to $c(J)$ and the geometric Picard number $\rho(X_{\bar{k}})$ in the following three cases:

- (a) $c(J) > 0$, which allows us to use Proposition 4.13.
- (b) $c(J) \leq 0$ and $\rho(X_{\bar{k}}) < 20$. In this case, X is a Kummer surface [Has03, Remark 9.7].
- (c) $\rho(X_{\bar{k}}) = 20$, that is, X is *singular* in the context of Shioda and Inose [SI77].

Proof of Theorem 4.14 for case (a). By Proposition 4.13, there exists an extension L/k of degree at most $48^2 \mathbf{c}_{20}$ and a non-torsion rational multisection $\mathcal{M} \subset X_L$ defined over L . The normalization of \mathcal{M} is a smooth rational curve, hence, upon replacing L by a quadratic extension of itself if necessary, we can assume that $\mathcal{M}(L)$ is dense in \mathcal{M} . Now we have

$$[L : k] \leq 2 \cdot 48^2 \mathbf{c}_{20} = 4608 \mathbf{c}_{20}.$$

Note that \mathcal{M} defines a rational map $\varphi: X \dashrightarrow J := J(X)$ by sending a point $x \in X_{\bar{k}}$ lying on a smooth fiber to

$$\varphi(x) := d_{\mathcal{M}}[x] - [\mathcal{M}_{\pi(x)}] \in \text{Pic}^0(X_{\pi(x)})$$

where $d_{\mathcal{M}}$ is the degree of \mathcal{M} .

By Merel's theorem (see, e.g. [Sil09, VIII, Theorem 7.5.1]), there exists a constant N depending only on $[L : \mathbb{Q}]$ such that every elliptic curve E over L satisfies $|E_{\text{tor}}(L)| \leq N$. For every positive integer n , the torsion points of order n on the fibers of $J_{\bar{k}}$ form a multisection $\mathcal{T}_n \subset J$. Let us define

$$\mathcal{T} := \bigcup_{n \leq N} \mathcal{T}_n \subset J.$$

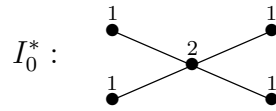
Since \mathcal{M} is non-torsion, there exist $x, y \in \mathcal{M}(L)$ lying on the same smooth fiber $X_{\pi(x)}$ such that $[x] - [y] \in \text{Pic}^0(X_{\pi(x)})$ is non-torsion. It follows that

$$\varphi(x) - \varphi(y) = d_{\mathcal{M}}([x] - [y]) \in J_{\pi(x)}$$

is also non-torsion. This implies that $\varphi(\mathcal{M})$ is not contained in \mathcal{T} , so the intersection $\varphi(\mathcal{M}) \cap T$ is zero-dimensional and thus contains only finitely many closed points. Hence, for all but finitely many $z \in \mathcal{M}(L)$, the image $\varphi(z) \in \varphi(\mathcal{M}(L))$ is either of infinite order or torsion of order greater than N . The latter case is impossible due to Merel's theorem. Thus for all but finitely many $z \in \mathcal{M}(L)$, the fiber $J_{\pi(z)}$ has infinitely many L -points. Translating points in $\mathcal{M}(L)$ by points in $J_{\pi(z)}$ gives a dense subset of L -points on X_L . \square

Remark 4.15. The strategy in the second part of the proof of case (a) has been used previously in literature to prove the density of rational points on surfaces that admits multiple elliptic fibrations over number fields. See, for example, [vL12, §3], where a more general result was proved.

Proof of Theorem 4.14 for case (b). By [Has03, Proposition 9.6], the fibration $X \rightarrow \mathbb{P}^1$ is isotrivial with four degenerate fibers of type I_0^* , represented by the diagram



The locus $B \subset \mathbb{P}^1$ under the degenerate fibers determines a double cover $E \rightarrow \mathbb{P}^1$ branched at B . The fiber product $X \times_{\mathbb{P}^1} E$ is non-normal along the preimages of the non-reduced components of the degenerate fibers. Its normalization, denoted as \tilde{Y} , contains sixteen (-1) -curves that are the preimages of the reduced components of the degenerate fibers. By contracting these (-1) -curves, we obtain an isotrivial elliptic fibration $f: Y \rightarrow E$ with smooth fibers. Let us organize these into a diagram:

$$\begin{array}{ccccc} & & \tilde{Y} & & \\ & & \downarrow & & \\ Y & \xleftarrow{\sim} & X \times_{\mathbb{P}^1} E & \xrightarrow{2:1} & X \\ \downarrow f & & \downarrow & & \downarrow \\ E & \xlongequal{\quad} & E & \xrightarrow{2:1} & \mathbb{P}^1. \end{array}$$

We claim that Y is a *hyperelliptic surface* in the sense of [BM77, §3], that is, its Kodaira dimension $\kappa(Y)$ is zero and the Albanese variety $\text{Alb}(Y)$ is an elliptic curve. First of all, one can verify that $\chi(Y) = 0$ by tracking the construction of Y . Together with the fact that $K_Y^2 = 0$ for an elliptic surface in general, we obtain $\chi(\mathcal{O}_Y) = 0$ by Noether's formula. Plugging this into [BM77, Theorem 2 (iv)], we conclude that the canonical bundle ω_Y of Y is the pullback of a line bundle \mathcal{L} on E of degree zero. Hence

$$\dim H^0(Y, \omega_Y^{\otimes m}) = \dim H^0(E, \mathcal{L}^{\otimes m}) = 1 \quad \text{for } m \gg 0.$$

This shows that $\kappa(Y) = 0$. On the other hand, the second Betti number of Y equals $b_2(Y) = b_2(E) = 2$ [CD89, Corollary 5.2.2], so the irregularity $q(Y) = b_2(Y)/2 = 1$. Thus $\text{Alb}(Y)$ has dimension one, that is, is an elliptic curve. This proves the claim.

Because E is a double cover of \mathbb{P}^1 , there exists an extension L_1/k of degree at most 2 such that $E(L_1) \neq \emptyset$, or equivalently, E_{L_1} is an elliptic curve. By Corollary 3.3, there exists an extension L_2/L_1 of degree at most 2 such that $E(L_2)$ contains a non-torsion point p . In particular, the set $E(L_2)$ is infinite, which implies that Y_{L_2} is a finite quotient of $E_{L_2} \times E'$ for some elliptic curve E' over L_2 by [BM77, Theorem 4]. (Although [BM77] works over an algebraically closed field, the same arguments work over K assuming $E(K)$ is infinite.) Applying Corollary 3.3 to E' , we get an extension L/L_2 of degree at most 2 such that $E'(L)$ contains a non-torsion point p' . Then the point $(p, p') \in E_L \times E'_L$ is nondegenerate as it spans a subset whose projections onto E_L and E'_L are Zariski dense. In particular, the L -rational points are dense in $E_L \times E'_L$ and thus dense in Y_L , which implies that $X(L)$ is dense as well. About the degree of L/k ,

$$[L : k] = [L : L_2][L_2 : L_1][L_1 : k] \leq 2 \cdot 2 \cdot 2 = 8 < 4608\mathbf{c}_{20}.$$

This completes the proof for case (b). □

Proof of Theorem 4.14 for case (c). Assume that $\rho(X_{\bar{k}}) = 20$. By Lemma 4.4 and Proposition 4.5, there exists a finite extension L/k of degree at most $48\mathbf{c}_{20}$ such that

- (i) $\text{Pic}(X_{\bar{k}}) \cong \text{Pic}(X_L)$, and
- (ii) every $f \in \text{Aut}(X_{\bar{k}})$ satisfies $f^n \in \text{Aut}(X_L)$ for some integer n .

Note that every elliptic fibration on $X_{\bar{k}}$ is defined over L due to (i). According to [SI77, §5], there exists an elliptic fibration

$$\pi : X_L \longrightarrow \mathbb{P}^1$$

which admits infinitely many sections over \bar{k} . In other words, the generic fiber X_η , as a genus one curve over $L(\mathbb{P}^1)$, contains infinitely many rational points over $K := \bar{k}(\mathbb{P}^1)$. Consider X_η as an elliptic curve over K . The Mordell–Weil theorem implies that $X_\eta(K)$ is finitely generated, so there exists $\Sigma \in X_\eta(K)$ that is non-torsion. Translation by Σ induces an automorphism $\sigma \in \text{Aut}(X_{\bar{k}})$ of infinite order. Using (ii) above, we conclude that there exists an integer n such that

$$\tau := \sigma^n \in \text{Aut}(X_L)$$

which is again of infinite order. Note that τ can also be considered as an automorphism on the genus one curve X_η .

By Lemma 4.12, after an extension L'/L of degree at most 48, there exists a rational multisection \mathcal{M} over L' . Extending by a quadratic extension if necessary, we can assume that $\mathcal{M}(L')$ is infinite. Let $\mathcal{M}' \cong \mathbb{P}^1_{L'}$ be the normalization of \mathcal{M} and consider the base change

$$\begin{array}{ccc} \tilde{X} := \mathcal{M}' \times_{\mathbb{P}^1} X_{L'} & \longrightarrow & X_{L'} \\ \downarrow & & \downarrow \pi \\ \mathcal{M}' & \longrightarrow & \mathbb{P}^1. \end{array}$$

Let ξ denote the generic point of \mathcal{M}' . Then the generic fiber \widetilde{X}_ξ can be seen as an elliptic curve since \widetilde{X} admits a section

$$\widetilde{\mathcal{M}} := \mathcal{M}' \times_{\mathbb{P}^1} \mathcal{M}.$$

Moreover, τ induces an automorphism $\widetilde{\tau}$ on \widetilde{X} of infinite order that acts on \widetilde{X}_ξ as an automorphism of a genus one curve.

The orbit of $\widetilde{\mathcal{M}}_\xi$ as a point on \widetilde{X}_ξ under $\widetilde{\tau}$ is infinite. Indeed, if not, then $\widetilde{\tau}^\ell(\widetilde{\mathcal{M}}_\xi) = \widetilde{\mathcal{M}}_\xi$ for some integer ℓ , hence τ^ℓ acts as an automorphism on the elliptic curve $(\widetilde{X}_\xi, \widetilde{\mathcal{M}}_\xi)$. However, the automorphism group of an elliptic curve is finite [Sil09, III, Theorem 10.1], which implies that $\widetilde{\tau}$ is of finite order, contradiction. As a consequence, the orbit of $\widetilde{\mathcal{M}}_\xi$ is infinite. It follows that the orbit of the set $\widetilde{\mathcal{M}}(L')$ under $\widetilde{\tau}$ is dense in \widetilde{X} . This produces a dense subset of L' -rational points on $X_{L'}$ via the morphism $\widetilde{X} \rightarrow X_{L'}$. Note that

$$[L' : k] = [L' : L][L : k] \leq 2 \cdot 48^2 \cdot \mathbf{c}_{20} = 4608\mathbf{c}_{20}$$

so we finish the proof. \square

5 Brauer groups and uniform potential density

In this section, we show that uniform potential density holds for a collection of varieties provided that certain conjectures related to the Brauer–Manin obstruction hold.

5.1 Brauer–Manin obstructions and related conjectures

For a comprehensive introduction to the Brauer–Manin obstruction, we refer the reader to [Poo17, Chapter 8]. Let us recall only necessary definitions here. Given a smooth and geometrically integral variety X over a number field k , we consider its Brauer group $\mathrm{Br}(X)$ and the following groups

$$\begin{aligned} \mathrm{Br}_0(X) &:= \mathrm{im}(\mathrm{Br}(k) \longrightarrow \mathrm{Br}(X)) \\ \mathrm{Br}_1(X) &:= \ker(\mathrm{Br}(X) \longrightarrow \mathrm{Br}(X_{\bar{k}})). \end{aligned}$$

Let Ω_k be the set of places of k . Each $v \in \Omega_k$ induces a homomorphism

$$\mathrm{inv}_v : \mathrm{Br}(k_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

called a *local invariant*. It is an isomorphism if v is finite, identifies $\mathrm{Br}(k_v)$ with $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if v is real, and is the zero map if v is complex. Using this, we can define the *adelic Brauer–Manin pairing*

$$\begin{aligned} \mathrm{Br}(X) \times X(\mathbb{A}_k) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (\alpha, \{x_v\}) &\longmapsto \sum_{v \in \Omega_k} \mathrm{inv}_v(\alpha(x_v)). \end{aligned} \tag{5.1}$$

This pairing is trivial on $\mathrm{Br}_0(X)$, so it can be considered as a pairing between $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ and $X(\mathbb{A}_k)$ as well. The subset in $X(\mathbb{A}_k)$ orthogonal to all elements in $\mathrm{Br}(X)$ under this pairing is denoted as $X(\mathbb{A}_k)^{\mathrm{Br}}$.

Let $\mathcal{C} = \{(X, k)\}$ be a collection of smooth and geometrically integral varieties X over number fields k . Recall that \mathcal{C} satisfies

- *uniform boundedness of exponent for Brauer groups (UBEB)* if, for every integer $d > 0$, there exists a constant c_d such that $c_d\alpha = 0$ for all $\alpha \in \text{Br}(X_L)/\text{Br}_0(X_L)$ where $X/k \in \mathcal{C}$ and L/k is an extension such that $[L : k] \leq d$;
- *Brauer–Manin obstruction is the only one to weak approximation (BMWA)* if for all $X/k \in \mathcal{C}$ and finite extension L/k , we have $X(L)$ dense in $X(\mathbb{A}_L)^{\text{Br}}$.
- *Uniform potential local solubility (UPLS)* if, there exists a constant c such that for all $X/k \in \mathcal{C}$, there exists an extension L/k of degree $\leq c$ such that X_L is everywhere locally soluble.

For example, the collection \mathcal{C} of geometrically rational surfaces over number fields satisfies UBEB since this holds for del Pezzo surfaces (see, e.g., [Cor07, Theorem 4.1] for a list of possible Brauer groups for del Pezzo surfaces) and conic bundles (see, e.g., [CTS19, Lemma 10.2.2 and Proposition 10.2.3]). It is conjectured by Colliot-Thélène that if \mathcal{C} consists of rationally connected variety defined over number fields, then \mathcal{C} satisfies BMWA [CT03, p.174]. Evidently, uniform potential density for \mathcal{C} implies UPLS.

For K3 surfaces over number fields, Skorobogatov-Zarhin [SZ08, Theorem 1.2] proved that $\text{Br}(X)/\text{Br}_0(X)$ is always finite. Drawing analogy from Merel’s theorem for elliptic curves, Várilly-Alvarado [VA17] further conjectured that a stronger condition than UBEB holds when restricted to families of K3 surfaces based on the lattice structures of their Néron–Severi groups. See also [OS18], [CC20], and [OSZ19] for some progress toward this conjecture.

Conjecture 5.1 ([VA17, Conjecture 4.6]). *Fix an integer $d > 0$ and a primitive lattice Δ in the K3 lattice $\Lambda_{K3} := U^{\oplus 3} \oplus E_8(-1)^{\oplus 2}$. Let $\mathcal{C} = \{(X, k)\}$ be the collection of K3 surfaces X over number fields k satisfying $\text{Pic}(X_{\bar{k}}) \simeq \Delta$ and $[k : \mathbb{Q}] \leq d$. Then there exists a constant c_d such that $|\text{Br}(X)/\text{Br}_0(X)| < c_d$ for any $X/k \in \mathcal{C}$;*

For BMWA, we have the following conjecture by Skorobogatov.

Conjecture 5.2 ([Sko09]). *K3 surfaces over a number fields satisfy BMWA.*

This conjecture was proved in the special case of Kummer surfaces assuming the finiteness of the relevant Tate–Shafarevich groups [SSD05]. It is far from being proved in general, but various computations have been done to support it, see, for example [Bri06].

5.2 A sufficient condition for uniform potential density

Our main result in this section relates UBEB, BMWA, and UPLS to uniform potential density. We first show that one can control the growth of Brauer groups using UBEB. Many variants of the following lemma have appeared in the literature; see Remark 5.4.

Lemma 5.3. *Let X be a smooth projective geometrically integral variety over a number field k such that $\text{Pic}(X_{\bar{k}})$ is torsion free of finite rank, and that UBEb holds for X . For any integer d , there exists an extension L/k such that for any extension K/k of degree d linearly disjoint from L , the natural map*

$$\text{Br}(X)/\text{Br}_0(X) \longrightarrow \text{Br}(X_K)/\text{Br}_0(X_K)$$

is an isomorphism.

Proof. Since $P := \text{Pic}(X_{\bar{k}})$ is finitely generated, the action by $\text{Gal}(\bar{k}/k)$ on P factors through a finite quotient, say $\text{Gal}(L/k)$. Since $\text{Gal}(\bar{k}/L)$ acts trivially on P , we have $H^1(L, P) = 0$. By the inflation restriction exact sequence,

$$H^1(\text{Gal}(L/k), P) \simeq H^1(k, P), \quad H^2(\text{Gal}(L/k), P) \hookrightarrow H^2(k, P). \quad (5.2)$$

Let $d > 0$ be an integer. By the hypothesis on UBEb, there exists a constant c_d such that for every extension M/k of degree at most d ,

$$\text{Br}(X_M)/\text{Br}_0(X_M)[c_d] = \text{Br}(X_M)/\text{Br}_0(X_M). \quad (5.3)$$

By [CTS19, Proposition 4.2.5], the set $\text{Br}(X_{\bar{k}})[c_d]$ is finite. Therefore, upon enlarging L by a finite extension if necessary, we can assume that $\text{Gal}(\bar{k}/L)$ acts trivially on $\text{Br}(X_{\bar{k}})[c_d]$. Let K/k be a degree d extension linearly disjoint from L/k . Then

$$\text{Br}(X_{\bar{k}})[c_d]^{\text{Gal}(\bar{k}/K)} = \text{Br}(X_{\bar{k}})[c_d]^{\text{Gal}(\bar{k}/k)} \quad (5.4)$$

The spectral sequence

$$E_2^{p,q} = H^p(k, H^q(X_{\bar{k}}, \mathbb{G}_m)) \implies H^{p+q}(X, \mathbb{G}_m)$$

gives rise to the following exact sequence (see e.g. [CTS13, Proposition 1.3 (i)])

$$0 \longrightarrow H^1(k, P) \longrightarrow \text{Br}(X)/\text{Br}_0(X) \longrightarrow \text{Br}(X_{\bar{k}})^{\text{Gal}(\bar{k}/k)} \longrightarrow H^2(k, P). \quad (5.5)$$

Enlarging L by a finite extension if necessary, we assume that the image of $\text{Br}(X_{\bar{k}})[c_d]^{\text{Gal}(\bar{k}/k)}$ lies in $H^2(\text{Gal}(L/k), P)$. Replacing $H^i(k, P)$ by $H^i(\text{Gal}(L/k), P)$ in (5.5) and taking the c_d -torsion elements in (5.5) gives the following commutative diagram by functoriality,

$$\begin{array}{ccccccc} H^1(\text{Gal}(L/k), P)[c_d] & \hookrightarrow & \frac{\text{Br}(X)}{\text{Br}_0(X)}[c_d] & \longrightarrow & \text{Br}(X_{\bar{k}})^{\text{Gal}(\bar{k}/k)}[c_d] & \longrightarrow & H^2(\text{Gal}(L/k), P) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(\text{Gal}(LK/K), P)[c_d] & \hookrightarrow & \frac{\text{Br}(X_K)}{\text{Br}_0(X_K)}[c_d] & \longrightarrow & \text{Br}(X_{\bar{k}})^{\text{Gal}(\bar{k}/K)}[c_d] & \longrightarrow & H^2(\text{Gal}(LK/K), P). \end{array}$$

Note that the first two rows of are exact because $\frac{\text{Br}(X)}{\text{Br}_0(X)}$ and $\frac{\text{Br}(X_K)}{\text{Br}_0(X_K)}$ are both c_d -torsion groups by assumption. From (5.4), we know that the third vertical map is an isomorphism. The first and last vertical map is an isomorphism since $\text{Gal}(L/k) \simeq \text{Gal}(LK/K)$ compatible with the action on P . The third vertical map is an isomorphism on the c_d -torsion parts by (5.4). Then the five lemma implies that the second vertical map is an isomorphism on the c_d -torsion parts, from which we deduce it is an isomorphism on the entire group by (5.3). \square

Remark 5.4. Special cases of Lemma 5.3 have appeared in the literature for varieties where UBEB is known. In [Lia13] and [Har97], the authors assumed the finiteness of the geometric Brauer group $\text{Br}(X_{\bar{k}})$. Ieronymou [Ier21] proved it for K3 surfaces X , in which case it follows from [OS18] that the X satisfies UBEB.

Theorem 5.5. *Let \mathcal{C} be a collection of smooth projective geometrically integral varieties X/k over number fields such that $H^1(X, \mathcal{O}_X) = 0$ and $\text{Pic}(X_{\bar{k}})$ is torsion-free of bounded rank. If \mathcal{C} satisfies UBEB, BMWA, and UPLS then it also satisfies uniform potential density.*

Proof. Using UPLS, up to a bounded extension of k , we can assume that X_k is everywhere locally soluble. By UBEB, there exists an integer N such that for any $X/k \in \mathcal{C}$, we have

$$N(\text{Br}(X)/\text{Br}_0(X)) = 0.$$

As a corollary to Lemma 5.3, there exists an extension K/k of degree N such that

$$\text{Br}(X)/\text{Br}_0(X) \longrightarrow \text{Br}(X_K)/\text{Br}_0(X_K) \quad (5.6)$$

is surjective.

We now show that $X(\mathbb{A}_K)^{\text{Br}} \neq \emptyset$. Let $\alpha \in \text{Br}(X_K)$. By (5.6), there exists $\beta \in \text{Br}(X)$ that maps to α modulo $\text{Br}_0(X_K)$. Since the Brauer–Manin pairing is trivial on $\text{Br}_0(X_K)$, we can assume without loss of generality that the image of β is in fact α . If $w \in \Omega_K$ is a place lying over $v \in \Omega_k$, then denote $e_w = [K_w : k_v]$. For any point $x_v \in X(k_v)$ with image $x_w \in X(K_w)$, we have the following commutative diagram.

$$\begin{array}{ccccc} \text{Br}(X_{k_v}) & \xrightarrow{x_v^*} & \text{Br}(k_v) & \xrightarrow{\text{inv}_v} & \mathbb{Q}/\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \times e_w \\ \text{Br}(X_{K_w}) & \xrightarrow{x_w^*} & \text{Br}(K_w) & \xrightarrow{\text{inv}_w} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Let $(x_v) \in X(\mathbb{A}_k)$ with image $(x_w) \in X(\mathbb{A}_K)$. Using the diagram above, we have

$$\begin{aligned} \sum_{w \in \Omega_K} \text{inv}_w \alpha(x_w) &= \sum_{v \in \Omega_k} \sum_{w|v} \text{inv}_w \alpha(x_w) \\ &= \sum_{v \in \Omega_k} \sum_{w|v} e_w \text{inv}_v \beta(x_v) \\ &= \sum_{v \in \Omega_k} N \text{inv}_v \beta(x_v) = 0. \end{aligned}$$

The last equality follows from the fact that $N\beta \in \text{Br}_0(X)$. So $(x_w) \in X(\mathbb{A}_K)^{\text{Br}}$ by the Brauer–Manin pairing (5.1). Our hypothesis on BMWA says that $X(K)$ is dense in $X(\mathbb{A}_K)^{\text{Br}}$. In the exact sequence

$$0 \longrightarrow \text{Br}_1(X_K)/\text{Br}_0(X_K)[N] \longrightarrow \text{Br}(X_K)/\text{Br}_0(X_K)[N] \longrightarrow \text{Br}(X_{\bar{k}})[N] \longrightarrow 0,$$

we have that $\text{Br}(X_{\bar{k}})[N]$ is finite by [CTS19, Proposition 4.2.5] and $\text{Br}_1(X)/\text{Br}_0(X) \simeq H^1(K, \text{Pic}(X_{\bar{k}}))$ is finite since $\text{Pic}(X_{\bar{k}})$ is torsion free of finite rank. Hence, $\text{Br}(X_K)/\text{Br}_0(X_K)$ is finite, which implies that $X(\mathbb{A}_K)^{\text{Br}}$ is a non-empty open subset in $X(\mathbb{A}_K)$ in the adelic topology. Hence $X(K)$ must be Zariski dense. \square

Corollary 5.6. *Fix a primitive lattice $L \subset \Lambda_{K3}$ and integer $d > 0$. Let $\mathcal{C} = \{(X, k)\}$ be the collection of all K3 surfaces X over number fields k that are everywhere locally soluble, satisfying $\text{Pic}(X_{\bar{k}}) \simeq L$ and $[k : \mathbb{Q}] \leq d$. Assume Conjectures 5.1 and 5.2. Then \mathcal{C} satisfies uniform potential density.*

Proof. Apply Theorem 5.5 since K3 surfaces satisfy $H^1(X, \mathcal{O}_X) = 0$ and $\text{Pic}(X_{\bar{k}})$ is torsion-free of bounded rank. \square

References

- [Bar55] I. Barsotti, *Un teorema di struttura per le varietà grupicali*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8) **18** (1955), 43–50.
- [BM77] E. Bombieri and D. Mumford, *Enriques’ classification of surfaces in char. p. II*, Complex analysis and algebraic geometry, 1977, pp. 23–42.
- [Bor91] A. Borel, *Linear algebraic groups*, Second, Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.
- [Bri06] M. Bright, *Brauer groups of diagonal quartic surfaces*, J. Symbolic Comput. **41** (2006), no. 5, 544–558.
- [BS16] L. Bary-Soroker, *Infiniteness of the galois cohomology over a number field with coefficients in a finite galois module*, 2016. <https://mathoverflow.net/q/239636>, an answer dated on May 24, 2016, to a MathOverflow post.
- [BT00] F. A. Bogomolov and Yu. Tschinkel, *Density of rational points on elliptic K3 surfaces*, Asian J. Math. **4** (2000), no. 2, 351–368.
- [BT72] A. Borel and J. Tits, *Compléments à l’article: “Groupes réductifs”*, Inst. Hautes Études Sci. Publ. Math. **41** (1972), 253–276.
- [CC20] A. Cadoret and F. Charles, *A remark on uniform boundedness for Brauer groups*, Algebr. Geom. **7** (2020), no. 5, 512–522.
- [CD89] F. R. Cossec and I. V. Dolgachev, *Enriques surfaces. I*, Progress in Mathematics, vol. 76, Birkhäuser Boston, Inc., Boston, MA, 1989.
- [CGP15] B. Conrad, O. Gabber, and G. Prasad, *Pseudo-reductive groups*, Second, New Mathematical Monographs, vol. 26, Cambridge University Press, Cambridge, 2015.
- [Che60] C. Chevalley, *Une démonstration d’un théorème sur les groupes algébriques*, J. Math. Pures Appl. (9) **39** (1960), 307–317.
- [Con02] B. Conrad, *A modern proof of Chevalley’s theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18.
- [Cor07] P. Corn, *The Brauer-Manin obstruction on del Pezzo surfaces of degree 2*, Proc. Lond. Math. Soc. (3) **95** (2007), no. 3, 735–777.
- [CT03] J.-L. Colliot-Thélène, *Points rationnels sur les fibrations*, Higher dimensional varieties and rational points (Budapest, 2001), 2003, pp. 171–221.
- [CTS13] J.-L. Colliot-Thélène and A. N. Skorobogatov, *Descente galoisienne sur le groupe de Brauer*, J. Reine Angew. Math. **682** (2013), 141–165.

- [CTS19] ———, *The Brauer–Grothendieck group*, 2019. <http://www.imperial.ac.uk/~anskor/brauer.pdf>.
- [EvdGM20] B. Edixhoven, G. van der Geer, and B. Moonen, *Abelian Varieties*, 2020. Online access at <https://www.math.ru.nl/~bmoonen/research.html>.
- [FJ08] M. D. Fried and M. Jarden, *Field arithmetic*, Third, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden.
- [GS17] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 165, Cambridge University Press, Cambridge, 2017.
- [Har97] D. Harari, *Flèches de spécialisations en cohomologie étale et applications arithmétiques*, Bull. Soc. Math. France **125** (1997), no. 2, 143–166.
- [Has03] B. Hassett, *Potential density of rational points on algebraic varieties*, Higher dimensional varieties and rational points (Budapest, 2001), 2003, pp. 223–282.
- [HT00] B. Hassett and Y. Tschinkel, *Abelian fibrations and rational points on symmetric products*, Internat. J. Math. **11** (2000), no. 9, 1163–1176.
- [Huy16] D. Huybrechts, *Lectures on K3 surfaces*, Cambridge Studies in Advanced Mathematics, vol. 158, Cambridge University Press, Cambridge, 2016.
- [Ier21] E. Ieronymou, *The Brauer–Manin obstruction for zero-cycles on K3 surfaces*, Int. Math. Res. Not. IMRN **3** (2021), 2250–2260.
- [Kan94] E. Kani, *Elliptic curves on abelian surfaces*, Manuscripta Math. **84** (1994), no. 2, 199–223.
- [Kol02] J. Kollár, *Unirationality of cubic hypersurfaces*, J. Inst. Math. Jussieu **1** (2002), no. 3, 467–476.
- [KP02] J. Kuzmanovich and A. Pavlichenkov, *Finite groups of matrices whose entries are integers*, Amer. Math. Monthly **109** (2002), no. 2, 173–186.
- [Lia13] Y. Liang, *Arithmetic of 0-cycles on varieties defined over number fields*, Ann. Sci. Éc. Norm. Supér. (4) **46** (2013), no. 1, 35–56 (2013).
- [LLR04] Q. Liu, D. Lorenzini, and M. Raynaud, *Néron models, Lie algebras, and reduction of curves of genus one*, Invent. Math. **157** (2004), no. 3, 455–518. [See corrigendum in: 3858404].
- [Maz00] B. Mazur, *Abelian varieties and the Mordell–Lang conjecture*, Model theory, algebra, and geometry, 2000, pp. 199–227.
- [Mil17] J. S. Milne, *Algebraic groups*, Cambridge Studies in Advanced Mathematics, vol. 170, Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.
- [Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.
- [Min87] H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, J. Reine Angew. Math. **101** (1887), 196–202.
- [OS18] M. Orr and A. N. Skorobogatov, *Finiteness theorems for K3 surfaces and abelian varieties of CM type*, Compos. Math. **154** (2018), no. 8, 1571–1592.
- [OSZ19] M. Orr, A. N. Skorobogatov, and Y. Zarhin, *On uniformity conjectures for abelian varieties and K3 surfaces*, American Journal of Mathematics (2019). <http://hdl.handle.net/10044/1/89834>.
- [Pie12] M. Pieropan, *On the unirationality of Del Pezzo surfaces over an arbitrary field*, Master’s Thesis, 2012. Accessible online at June 23, 2021 via: <https://algant.eu/documents/theses/pieropan.pdf>.
- [Poo17] B. Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017.

- [Ros56] M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443.
- [RY01] Z. Reichstein and B. Youssin, *Splitting fields of G -varieties*, Pacific J. Math. **200** (2001), no. 1, 207–249.
- [San81] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. Reine Angew. Math. **327** (1981), 12–80.
- [SI77] T. Shioda and H. Inose, *On singular $K3$ surfaces*, Complex analysis and algebraic geometry, 1977, pp. 119–136.
- [Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
- [Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
- [Sko09] A. N. Skorobogatov, *Diagonal quartic surfaces*, Oberwolfach Reports **33** (2009), 76–79.
- [SSD05] A. N. Skorobogatov and P. Swinnerton-Dyer, *2-descent on elliptic curves and rational points on certain Kummer surfaces*, Adv. Math. **198** (2005), no. 2, 448–483.
- [Ste65] R. Steinberg, *Regular elements of semisimple algebraic groups*, Inst. Hautes Études Sci. Publ. Math. **25** (1965), 49–80.
- [STVA14] C. Salgado, D. Testa, and A. Várilly-Alvarado, *On the unirationality of del Pezzo surfaces of degree 2*, J. Lond. Math. Soc. (2) **90** (2014), no. 1, 121–139.
- [SvL14] C. Salgado and R. van Luijk, *Density of rational points on del Pezzo surfaces of degree one*, Adv. Math. **261** (2014), 154–199.
- [SZ08] A. N. Skorobogatov and Y. G. Zarhin, *A finiteness theorem for the Brauer group of abelian varieties and $K3$ surfaces*, J. Algebraic Geom. **17** (2008), no. 3, 481–502.
- [Tit92] J. Tits, *Sur les degrés des extensions de corps déployant les groupes algébriques simples*, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), no. 11, 1131–1138.
- [Tot04] B. Totaro, *Splitting fields for E_8 -torsors*, Duke Math. J. **121** (2004), no. 3, 425–455.
- [VA13] A. Várilly-Alvarado, *Arithmetic of del Pezzo surfaces*, Birational geometry, rational curves, and arithmetic, 2013, pp. 293–319.
- [VA17] ———, *Arithmetic of $K3$ surfaces*, Geometry over nonclosed fields, 2017, pp. 197–248.
- [vL12] R. van Luijk, *Density of rational points on elliptic surfaces*, Acta Arith. **156** (2012), no. 2, 189–199.

K.-W. Lai, DEPARTMENT OF MATHEMATICS & STATISTICS
 UNIVERSITY OF MASSACHUSETTS
 AMHERST, MA 01003, USA
 lai@math.umass.edu

M. Nakahara, DEPARTMENT OF MATHEMATICS
 UNIVERSITY OF WASHINGTON
 SEATTLE, WA 98195, USA
 mn75@uw.edu