

THE d -PRIMARY BRAUER-MANIN OBSTRUCTION FOR CURVES

BRENDAN CREUTZ, BIANCA VIRAY, AND JOSÉ FELIPE VOLOCH

ABSTRACT. For a curve over a global field we consider for which integers d the d -primary part of the Brauer group can obstruct the existence of rational points. We give examples showing it is possible that there is a d -primary obstruction for infinitely many relatively coprime d , and also an example where the odd part of the Brauer group does not obstruct although there is a Brauer-Manin obstruction. These examples demonstrate that a slightly stronger form of a conjecture of Poonen is false, despite being supported by the same heuristic.

1. INTRODUCTION

Let k be a global field, \mathbb{A}_k its ring of adèles and let X be a smooth projective and geometrically integral variety over k . Manin observed that any adelic point $(P_v) \in X(\mathbb{A}_k)$ that is approximated by a k -rational point must satisfy relations imposed by elements of $\text{Br } X := H_{\text{ét}}^2(X, \mathbb{G}_m)$, the Brauer group of X [Man71]. More precisely, there is a pairing $X(\mathbb{A}_k) \times \text{Br } X \rightarrow \mathbb{Q}/\mathbb{Z}$ such that, for each element $\alpha \in \text{Br } X$, the set $X(\mathbb{A}_k)^\alpha$ of adelic points pairing trivially with α is closed and contains the k -rational points of X . In particular, for any subset $B \subset \text{Br } X$ the implication

$$(1.1) \quad X(\mathbb{A}_k)^B := \bigcap_{\alpha \in B} X(\mathbb{A}_k)^\alpha = \emptyset \quad \implies \quad X(k) = \emptyset.$$

always holds. When $X(\mathbb{A}_k)^{\text{Br}} = \emptyset$ one says there is a Brauer-Manin obstruction to the existence of rational points. Here and below $X(\mathbb{A}_k)^{\text{Br}}$ is used to denote $X(\mathbb{A}_k)^{\text{Br } X}$.

It is an outstanding open question, first raised by Skorobogatov [Sko01, p. 133] in the number field case, whether this is the only obstruction for $X = C$ a curve. Poonen [Poo06] and Stoll [Sto07] have conjectured an affirmative answer to this question. This has been proved for curves over function fields, under additional but quite general hypotheses [PV10].

Computation of the set $C(\mathbb{A}_k)^{\text{Br}}$ is quite difficult, in part because the Brauer group of a curve over a global field is quite large. Modulo constant algebras there are infinitely many elements of order n for every integer n . However, in any case where $C(\mathbb{A}_k)^{\text{Br}} = \emptyset$, there is an integer d such that $C(\mathbb{A}_k)^{\text{Br } C[d]} = \emptyset$, where $\text{Br } C[d]$ denotes the d -torsion subgroup. In fact, more is true. A simple compactness argument shows that, if $C(\mathbb{A}_k)^{\text{Br}} = \emptyset$, then there exists a finite subgroup B of $\text{Br } C$ with $C(\mathbb{A}_k)^B = \emptyset$ (see, e.g., [CV17, Lemma 4.8]). In this paper, we investigate what one can determine about such a subgroup *a priori* and, in particular, which integers d allow for a d -primary Brauer-Manin obstruction, i.e., there is such a subgroup $B \subset \text{Br } C$ consisting of elements that are annihilated by some power of d . Knowledge of such subgroups can facilitate computation Brauer-Manin obstructions in practice and may shed

The second author was partially supported by NSF CAREER grant DMS-1553459 and a University of Canterbury Visiting Erskine Fellowship. The third author acknowledges support from the Simons Foundation via the Collaboration Grant #234591.

light on the nature of the Brauer-Manin obstruction itself. In addition, if the conjecture is false, having such an a-priori hold on a subgroup B opens the possibility of producing an explicit counterexample.

If we assume finiteness of Tate-Shafarevich groups of abelian varieties, then it follows from Manin's arguments in [Man71] that any Brauer-Manin obstruction on a torsor under an abelian variety can be detected from the P -primary subgroup of the Brauer group, where P is the period of the torsor in question (i.e. its order in the Weil-Châtelet group). A stronger, unconditional statement along these lines is proved in [CV17]: if there is an d -primary Brauer-Manin obstruction for some integer d , then there is a $\gcd(d, P)$ -primary Brauer-Manin obstruction. Similar results are achieved in the case of Kummer varieties [CV17, SZ16], bielliptic surfaces (assuming finiteness of certain Tate-Shafarevich groups) [CV17], and fibrations of torsors under abelian varieties over projective space [Nak17] as well as minimal del Pezzo surfaces (by combining [Cor07, Nak17, SD93]; see [CV17]). Note that all cases considered thus far have non-maximal Kodaira dimension.

In this paper, we turn our attention to curves of genus at least 2, the simplest examples of varieties of maximal Kodaira dimension. Our results show that the situation here is quite different. We prove that there exist curves with a d -primary Brauer-Manin obstruction for infinitely many pairwise coprime integers d (Theorem 3.1). Given the well known connection between abelian descent and the Brauer-Manin obstruction, we even expect there to be locally soluble curves of general type with a p -primary Brauer-Manin obstructions for every prime p . We show, however, that this is not the case for all curves without rational points. For any prime p we construct a pointless curve of general type with no p -primary Brauer-Manin obstruction (Theorem 4.2). We also construct a pointless genus 3 curve C with a zero-cycle of degree 1 over \mathbb{Q} for which there is no odd Brauer-Manin obstruction (Theorem 4.1). This construction yields an infinite tower of non-isomorphic étale coverings of X in which all covers are counterexamples to the Hasse principle (Remark 4.4). Assuming finiteness of Tate-Shafarevich groups of elliptic curves, such towers cannot exist above genus 1 curves.

These examples have an interesting interpretation in relation to Poonen's heuristic [Poo06] for rational points on curves, one of the key pieces of evidence in support of (a strong form of) the conjecture that Brauer-Manin is the only obstruction for curves. Poonen shows that if, for all places v of k of good reduction for the Jacobian J of C , the set of rational points of C over the residue field \mathbb{F}_v viewed inside the group $J(\mathbb{F}_v)$ behaves like a random subset of the same cardinality and the order of $J(\mathbb{F}_v)$ is as smooth as a typical integer of the same size, then the conjecture holds with probability one. We show that the implication of Poonen's heuristic goes through if, instead of $J(\mathbb{F}_v)$, we take the quotient of $J(\mathbb{F}_v)$ by its d -primary subgroup for an integer d (Theorem 5.3). However, we show that the conclusion is false in examples such as those mentioned in the paragraph above. This suggests one should be careful putting too much faith in such heuristics.

Constant curves over global function fields are excluded by the hypotheses in [PV10] and are known to exhibit somewhat unusual behavior, e.g., the failure of Mordell's conjecture. It is thus unclear in this case whether one should even expect Brauer-Manin to be the only obstruction. In view of this, we have included constant curves in our investigations, producing several relevant examples and general results (e.g., Theorem 2.14 and Proposition 2.12).

Notation. A nice variety over a field K is a smooth, projective and geometrically integral K -variety. We will use *curve* to mean a nice variety of dimension 1. For a K -scheme X we use

\overline{X} to denote the base change of X to a separable closure \overline{K} of K and $\mathbf{k}(X)$ to denote the sheaf of total quotient rings. Note that for X integral, $\mathbf{k}(X)$ can be identified with the function field of X . We use $H^i(X, \bullet)$ to denote flat cohomology groups, and abbreviate $H^i(\mathrm{Spec} K, \bullet)$ to $H^i(K, \bullet)$. The Brauer group of a scheme X is $\mathrm{Br} X := H^2(X, \mathbb{G}_m)$. This agrees with the étale cohomology group $H_{\mathrm{ét}}^2(X, \mathbb{G}_m)$ as defined above [Mil80, Theorem III.3.9]. We use $\mathrm{Br}_1 X$ to denote the kernel of the map $\mathrm{Br} X \rightarrow \mathrm{Br} \overline{X}$ induced by base change.

Throughout the paper k denotes a global field. The set of places of k is denoted Ω_k . For $v \in \Omega_k$, the corresponding completion is k_v and, when v is finite, the residue field is \mathbb{F}_v . We use \mathbb{A}_k to denote the ring of adèles of k . For X a curve (resp. an abelian variety) over k we use $X_{\mathbb{F}_v}$ to denote the special fiber of the minimal proper regular model (resp. Néron model) of $X \times_k k_v$. When $X_{\mathbb{F}_v}$ is a nice \mathbb{F}_v -variety we often abuse notation by writing $X(\mathbb{F}_v)$ in place of $X_{\mathbb{F}_v}(\mathbb{F}_v)$.

For an integer d and an abelian group G (or group scheme), let $G[d^\infty]$ and $G[d^\perp]$ denote, respectively, the d -primary and prime-to- d torsion subgroups. Recall that a **supernatural number** is a formal product $\prod p^{n_p}$ ranging over all prime numbers p . We extend the notation $G[d^\infty]$ and $G[d^\perp]$ to supernatural numbers d in the obvious way. Namely $G[d^\infty] = \bigcup_{d_0 \in \mathbb{N}, d_0 | d} G[d_0^\infty]$ and $G[d^\perp] = \bigcap_{d_0 \in \mathbb{N}, d_0 | d} G[d_0^\perp]$. For any supernatural d and any torsion abelian group G we have a splitting $G \simeq G[d^\infty] \times G[d^\perp]$. We use pr_{d^∞} and pr_{d^\perp} to denote the corresponding projections.

ACKNOWLEDGEMENTS

This work was heavily based on discussions that took place at University of Canterbury while the second author was a visiting Erskine Fellow and at the Rational Points 2017 workshop. We thank the Erskine Programme for its support and Michael Stoll for his support as well as for a number of helpful comments.

2. PRELIMINARIES

2.1. Relating the Brauer-Manin obstruction, finite abelian descent, and divisibility on abelian varieties. Let X be a nice variety over a global field k with Albanese variety $A := \mathrm{Alb}_X^0$ and Picard variety $\hat{A} = \mathrm{Pic}_X^0$. For an integer $d \geq 2$, we define a d -covering of X to be an X -torsor under $\hat{A}[d]$ whose **type** (cf. [Sko01, Section 2.3]) is the inclusion $\lambda_d: \hat{A}[d](\overline{k}) \hookrightarrow \hat{A}(\overline{k}) = \mathrm{Pic}_X^0(\overline{k}) \rightarrow \mathrm{Pic} \overline{X}$. We define $X(\mathbb{A}_k)^{d\text{-ab}}$ to be the set of adelic points on X that lift to an adelic point on some d -covering of X . Recall that $X(k) \subset X(\mathbb{A}_k)^{d\text{-ab}}$.

From the Hochschild-Serre spectral sequence we have a map $\mathrm{Br}_1 X \rightarrow H^1(k, \mathrm{Pic} \overline{X})$ which induces an isomorphism $\mathrm{Br}_1 X / \mathrm{Br}_0 X \simeq H^1(k, \mathrm{Pic} \overline{X})$, since k a global field implies $H^3(k, \overline{k}^\times) = 0$ (cf. [NSW08, 8.3.11(iv) and 8.3.12]). The map λ_d induces maps

$$(2.1) \quad H^1(k, \hat{A}[d]) \rightarrow H^1(k, \hat{A}) \rightarrow H^1(k, \mathrm{Pic} \overline{X}).$$

We define $\mathrm{Br}_{1/2,d} X$ and $\mathrm{Br}_{1/2} X$ to be the subgroups of $\mathrm{Br}_1 X$ whose images in $H^1(k, \mathrm{Pic} \overline{X})$ lie in the images of $H^1(k, \hat{A}[d])$ and $H^1(k, \hat{A})$ under (2.1), respectively. The notation $\mathrm{Br}_{1/2} X$ was first introduced, in the number field case, in [Sto07]. To simplify the notation we write $X(\mathbb{A}_k)^{\mathrm{Br}_{1/2}}$ in place of $X(\mathbb{A}_k)^{\mathrm{Br}_{1/2} X}$ and similarly for $X(\mathbb{A}_k)^{\mathrm{Br}_{1/2,d}}$, etc.

Proposition 2.1. *Let A be an abelian variety over a global field k . Then $A(\mathbb{A}_k)^{\mathrm{Br}_{1/2,d}} = A(\mathbb{A}_k)^{d\text{-ab}}$.*

Proof. For k a number field, this is a special case of [Sko01, Theorem 6.1.2(a)]. This can be extended to global fields of positive characteristic as follows. The proof in the number field case involves three steps, as outlined at the top of page 115 of op. cit. The first step is to show the existence of an A -torsor of type λ_d . In our situation this is guaranteed since multiplication by d endows A with the structure of a d -covering. The second step of the proof (beginning on page 119 of op. cit.) is to prove the containment $A(\mathbb{A}_k)^{\text{Br}_{1/2,d}} \subset A(\mathbb{A}_k)^{d\text{-ab}}$, assuming the existence of an A -torsor of type λ_d . This follows from local Tate duality and the Poitou-Tate exact sequence. The proof carries through verbatim in the function field case, provided one uses the local duality statement [Mil06, III.6.10] in place of [Mil06, I.2.3] and the Poitou-Tate sequence [Čes15, Theorem 5.1] in place of [Mil06, I.4.20]. The third step of the proof is to show the containment $A(\mathbb{A}_k)^{d\text{-ab}} \subset A(\mathbb{A}_k)^{\text{Br}_{1/2,d}}$. This follows from functoriality of the Brauer pairing and the fact that for any A -torsor $\pi : Y \rightarrow A$ of type λ_d the induced map π^* annihilates $\text{Br}_{1/2,d} A / \text{Br}_0 A$. \square

Corollary 2.2. *Let A be an abelian variety over a global field k and let $(P_v) \in A(\mathbb{A}_k)$ be an adelic point. If there exists $Q \in A(k)$ such that $((P_v) - Q) \in dA(\mathbb{A}_k)$, then $(P_v) \in A(\mathbb{A}_k)^{\text{Br}_{1/2,d}}$. Conversely, if s is a positive integer such that $d^s \text{III}(k, A)[d^\infty] = 0$ and $(P_v) \in A(\mathbb{A}_k)^{\text{Br}_{1/2,d^n}}$ with $n - s \geq 0$, then there exists $Q \in A(k)$ such that $((P_v) - Q) \in d^{n-s} A(\mathbb{A}_k)$.*

Remark 2.3. *Let $A(\mathbb{A}_k)_\bullet = \prod \pi_0(A(k_v))$, where π_0 denotes the group of connected components. Note that $\pi_0(A(k_v)) = A(k_v)$ if v is not archimedean. It is known that the closure of the image of $A(k)$ in $A(\mathbb{A}_k)_\bullet$ is its profinite completion. From this and the previous lemma it follows that $\overline{A(k)} = A(\mathbb{A}_k)_\bullet^{\text{Br}}$ when $\text{III}(k, A)$ is finite. See [PV10, Remark 4.5].*

Proof. If $(P_v) - Q \in dA(\mathbb{A}_k)$, then (P_v) lifts to the d -covering $A \ni x \mapsto dx + Q \in A$, so $(P_v) \in A(\mathbb{A}_k)^{d\text{-ab}}$, which equals $A(\mathbb{A}_k)^{\text{Br}_{1/2,d}}$ by Proposition 2.1. Now suppose (P_v) is as in the second statement of the lemma. By Proposition 2.1, (P_v) survives d^n -descent, so there is a d^n -covering $\pi : Y \rightarrow A$ such that $(P_v) = \pi(Q_v)$ for some $(Q_v) \in Y(\mathbb{A}_k)$. The map π must factor as $Y \rightarrow Y' \rightarrow A$ where $Y' \rightarrow A$ is a d^{n-s} -covering. Moreover, the assumption that $d^s \text{III}(k, A) = 0$ implies that the class of Y' in $\text{III}(k, A)$ is trivial. Hence there is an isomorphism $Y' \simeq A$ identifying the map $Y' \rightarrow A$ with the map $A \rightarrow A$ given by $x \mapsto d^{n-s}x + Q$ for some $Q \in A(k)$. In particular, $((P_v) - Q) \in d^{n-s} A(\mathbb{A}_k)$. \square

2.2. Relating the Brauer-Manin obstruction, finite abelian descent, and divisibility on curves. This section is highly influenced by [Sto07]. In the number field case the results of this section can be found in or easily deduced from [Sto07, Sections 6 and 7]. Suppose C/k is a nice curve of genus at least 1 over a global field k . Let $J := \text{Jac}(C) = \text{Alb}_C^0 = \text{Pic}_C^0$ be its Jacobian. Suppose further that there exists a zero cycle z of degree 1 on C and that this is used to define an embedding $\iota : C \rightarrow J$ by the rule $x \mapsto [x - z]$.

Lemma 2.4. *The map ι induces surjective morphisms*

- (1) $\text{Br } J \rightarrow \text{Br } C$,
- (2) $\text{Br}_{1/2} J \rightarrow \text{Br } C$, and
- (3) $\text{Br}_{1/2,d} J \rightarrow \text{Br } C[d]$.

Proof. The existence of a zero-cycle of degree 1 implies that the exact sequence of Galois modules $0 \rightarrow \text{Pic}^0 \overline{C} \rightarrow \text{Pic } \overline{C} \rightarrow \mathbb{Z} \rightarrow 0$ is split and so induces an isomorphism

$H^1(k, \text{Pic}^0 \bar{C}) \simeq H^1(k, \text{Pic} \bar{C})$. Then we have a commutative diagram (with non-exact rows),

$$\begin{array}{ccccc} H^1(k, \text{Pic}^0 \bar{J}) & \longrightarrow & H^1(k, \text{Pic} \bar{J}) & \longrightarrow & \text{Br}_1 J / \text{Br}_0 J \\ \parallel \iota^* & & \downarrow \iota^* & & \downarrow \iota^* \\ H^1(k, \text{Pic}^0 \bar{C}) & \longrightarrow & H^1(k, \text{Pic} \bar{C}) & \longrightarrow & \text{Br}_1 C / \text{Br}_0 C \end{array}$$

The maps in the bottom row are all isomorphisms, so the vertical maps must all be surjective. By definition $\text{Br}_{1/2} J \subset \text{Br} J$ is the subgroup whose image lies in the image of $H^1(k, \text{Pic}^0 \bar{J})$. Furthermore, $\text{Br}_1 C = \text{Br} C$ by Tsen's theorem and the existence of a zero-cycle of degree 1 yields an isomorphism $\text{Br}_0 J \rightarrow \text{Br}_0 C$, so we have the surjectivity of (2). This shows that (1) is also surjective. Statement (3) follows from the surjectivity of the map $H^1(k, J[d]) \rightarrow H^1(k, J)[d] \simeq (\text{Br}_1 C / \text{Br}_0 C)[d]$. \square

Corollary 2.2, Lemma 2.4 and functoriality of the Brauer pairing yield the following.

Corollary 2.5. *For any integer d , $C(\mathbb{A}_k)^{d-ab} = C(\mathbb{A}_k)^{\text{Br} C[d]}$.*

Corollary 2.6. *Let $(P_v) \in C(\mathbb{A}_k)$. Then $(P_v) \in C(\mathbb{A}_k)^{\text{Br}}$ if and only if $\iota(P_v) \in J(\mathbb{A}_k)^{\text{Br}}$.*

Corollary 2.7. *Let $(P_v) \in C(\mathbb{A}_k)$ be an adelic point. If there exists $Q \in J(k)$ such that $(\iota(P_v) - Q) \in dJ(\mathbb{A}_k)$, then $(P_v) \in C(\mathbb{A}_k)^{\text{Br} C[d]}$. Conversely, if s is a positive integer such that $d^s \text{III}(k, J)[d^\infty] = 0$ and $(P_v) \in C(\mathbb{A}_k)^{\text{Br} C[d]}$ with $n - s \geq 0$, then there exists $Q \in J(k)$ such that $(\iota(P_v) - Q) \in d^{n-s} J(\mathbb{A}_k)$.*

Corollary 2.8. *If for each $n \geq 1$ there exists $Q_n \in J(k)$ such that $(\iota(P_v) - Q_n) \in d^n J(\mathbb{A}_k)$, then $(P_v) \in C(\mathbb{A}_k)^{\text{Br} C[d^\infty]}$. If $\text{III}(k, J)[d^\infty]$ is finite, then the converse holds.*

2.3. Relating the d -primary Brauer-Manin and Poonen-Scharaschkin sets on curves.

Let C be a curve over a global field k with z a zero-cycle of degree 1 on C . Let $\iota: C \hookrightarrow J$ be the embedding, $x \mapsto [x - z]$. For each prime v of k that is of good reduction for C (and hence J) use $r_v: J(k_v) \rightarrow J(\mathbb{F}_v)$ to denote the reduction map and let $r: J(\mathbb{A}_k) \rightarrow \prod_{v \text{ good}} J(\mathbb{F}_v)$ be the product of the r_v over all primes of good reduction.

For a supernatural number d , consider the following commutative diagram,

$$(2.2) \quad \begin{array}{ccccccc} C(k) & \xrightarrow{\iota} & J(k) & & & & \\ \downarrow & & \downarrow & \searrow r & & & \\ C(\mathbb{A}_k) & \xrightarrow{\iota} & J(\mathbb{A}_k) & \xrightarrow{r} & \prod_{v \text{ good}} J(\mathbb{F}_v) & \xrightarrow{\text{pr}_{d^\infty}} & \prod_{v \text{ good}} J(\mathbb{F}_v)[d^\infty]. \end{array}$$

Assuming finiteness of $\text{III}(k, J)$, Scharaschkin showed [Sch99, Theorem 3.1.1] that ι induces a bijection between $C(\mathbb{A}_k)^{\text{Br}}$ and the intersection of $\iota(C(\mathbb{A}_k))$ with the topological closure of $J(k)$ in $J(\mathbb{A}_k)$. He also considered the intersection after applying the map r as featured in the following definition. We extend this to consider the d -primary and prime-to- d parts.

Definition 2.9. *The Poonen-Scharaschkin set $C(\mathbb{A}_k)^{\text{PS}}$ is the subset of adelic points whose image under $r \circ \iota$ lands in the topological closure (with respect to the product of the discrete topologies) of $r(J(k))$ inside $\prod_{v \text{ good}} J(\mathbb{F}_v)$. Similarly, the d -primary Poonen-Scharaschkin set $C(\mathbb{A}_k)^{\text{PS}[d^\infty]}$ is the subset of adelic points whose image under $\text{pr}_{d^\infty} \circ r \circ \iota$ lands in the topological closure of $\text{pr}_{d^\infty}(r(J(k)))$ inside $\prod_v J(\mathbb{F}_v)[d^\infty]$.*

Proposition 2.10. *Suppose $\iota: C \rightarrow J$ is as above and d is an integer.*

- (1) *If $\text{III}(k, J)[d^\infty]$ is finite, then $C(\mathbb{A}_k)^{\text{Br}C[d^\infty]} \subset C(\mathbb{A}_k)^{\text{PS}[d^\infty]}$.*
- (2) *If $\text{III}(k, J)[d^\perp]$ is finite, then $C(\mathbb{A}_k)^{\text{Br}C[d^\perp]} \subset C(\mathbb{A}_k)^{\text{PS}[d^\perp]}$.*

Remark 2.11. *This proposition is a slightly refined version of Scharaschkin's result [Sch99] that if $\text{III}(k, J)$ is finite and $C(\mathbb{A}_k)^{\text{PS}} = \emptyset$, then $C(\mathbb{A}_k)^{\text{Br}C} = \emptyset$.*

Proof. It suffices to prove the first statement for d a supernatural integer. Let $(P_v) \in C(\mathbb{A}_k)^{\text{Br}C[d^\infty]}$. We will show that, for any finite set of places S of good reduction for J , there is some $Q \in J(k)$ such that (P_v) and Q have the same image in $\prod_{v \in S} J(\mathbb{F}_v)[d^\infty]$. Let e be the exponent of the finite group $\prod_{v \in S} J(\mathbb{F}_v)[d^\infty]$. By assumption $(P_v) \in C(\mathbb{A}_k)^{\text{Br}C[e^\infty]}$. Since $\text{III}(k, J)[e^\infty] \subset \text{III}(k, J)[d^\infty]$ is assumed to be finite, Corollary 2.8 yields the existence of some $Q \in J(k)$ such that $(\iota(P_v) - Q) \in eJ(\mathbb{A}_k)$. Then (P_v) and Q have the same image in $\prod_{v \in S} J(\mathbb{F}_v)[d^\infty]$, since e is the exponent of this group. \square

In the case of constant curves over global function fields, we have the following partial converse to Proposition 2.10.

Proposition 2.12. *Suppose C is a constant curve over a global function field k and $d \geq 1$ is an integer.*

- (1) *If $C(\mathbb{A}_k)^{\text{Br}C} = \emptyset$, then $C(\mathbb{A}_k)^{\text{PS}} = \emptyset$.*
- (2) *If $C(\mathbb{A}_k)^{\text{Br}C[d^\infty]} = \emptyset$, then $C(\mathbb{A}_k)^{\text{PS}[d^\infty]} = \emptyset$.*

The proof will require the following lemma.

Lemma 2.13. *Suppose X is a nice constant variety over a global function field k with constant field \mathbb{F}_q . Let $F: X \rightarrow X$ denote the \mathbb{F}_q -Frobenius. The sequence of functions $F^{n!}: X(\mathbb{A}_k) \rightarrow X(\mathbb{A}_k)$ converges uniformly to the "reduction map" $X(\mathbb{A}_k) \rightarrow X(\mathbb{A}_\mathbb{F}) := \prod X(\mathbb{F}_v) \subset X(\mathbb{A}_k)$.*

Proof. It is clear that the pointwise limit of the sequence is the reduction map. The sequence is equicontinuous, since for any $x, y \in X(\mathbb{A}_k)$ we have $\rho(x, y) \geq \rho(F(x), F(y))$, where ρ is any metric inducing the adelic topology. Uniform convergence then follows from the Arzelà-Ascoli theorem, which applies as $X(\mathbb{A}_k)$ is compact (e.g., [Roy88, Ch. 7, Lemma 39]). \square

Proof of Proposition 2.12. Enumerate the places of k and define S_m to be the set consisting of the first m of them. Note that every place $v \in \Omega_k$ is a place of good reduction since C is a constant curve. Suppose $(P_v) \in C(\mathbb{A}_k)^{\text{PS}}$. Then for each $m \geq 1$ there exist $Q_m \in J(k)$ such that $r_v(\iota(P_v)) = r_v(Q_m)$ in $J(\mathbb{F}_v)$, for all primes v in S_m . By Lemma 2.13 the limit $\lim_n F^{n!}(Q_n)$ exists and is equal to $\lim_n F^{n!}(\iota(P_v)) = r(\iota(P_v)) \in J(\mathbb{A}_\mathbb{F}) \subset J(\mathbb{A}_k)$. Thus, $r(\iota(P_v)) \in \overline{J(k)} \subset J(\mathbb{A}_k)^{\text{Br}}$. Since r commutes with ι , Corollary 2.8 implies that $r(P_v) \in C(\mathbb{A}_k)^{\text{Br}}$.

Now we prove the d -primary version. Assume $(P_v) \in C(\mathbb{A}_k)^{\text{PS}[d^\infty]}$. Then there exist $Q_n \in J(k)$ such that $Q_n - \iota(P_v)$ reduces to $J(\mathbb{F}_v)[d^\perp]$ for all $v \in S_n$. By Lemma 2.13, the limits $r(\iota(P_v)) = \lim_n F^{n!}(\iota(P_v))$ and $Q_0 := \lim_n F^{n!}Q_n$ exist and are equal after projecting to the d -primary subgroup of $J(\mathbb{A}_\mathbb{F}) = \prod J(\mathbb{F}_v)$. So $r(\iota(P_v)) - Q_0 \in J(\mathbb{A}_\mathbb{F})[d^\perp] \subset J(\mathbb{A}_k)[d^\perp]$. In particular, $r(\iota(P_v)) - Q_0 \in d^\infty J(\mathbb{A}_k)$. Also, $Q_0 \in \overline{J(k)} \subset J(\mathbb{A}_k)^{\text{Br}}$. Since $\text{III}(k, J)[d^\infty]$ is finite, Corollary 2.8 gives, for every n , some $R_n \in J(k)$ such that $Q_0 - R_n \in d^n J(\mathbb{A}_k)$. Thus we see that $(r(\iota(P_v)) - R_n) = (r(\iota(P_v)) - Q_0) - (Q_0 - R_n) \in d^n J(\mathbb{A}_k)$. It now follows from Corollary 2.8 and the commutativity of r and ι that $(r(P_v)) \in C(\mathbb{A}_k)^{\text{Br}C[d^\infty]}$. \square

2.4. Sufficiency of the Brauer-Manin obstruction on certain constant curves.

Theorem 2.14. *Let C be a curve defined over a finite field \mathbb{F} with $C(\mathbb{F}) = \emptyset$ and let k/\mathbb{F} be a function field such that $J(k)$ is not Zariski dense in J , the Jacobian of C . Then $C(\mathbb{A}_k)^{\text{Br}} = \emptyset$.*

Remark 2.15. *Note that in [PV10] it is shown that the Brauer-Manin obstruction is the only obstruction to weak approximation for curves over function fields satisfying additional, but quite general, hypotheses. One of these hypotheses, however, excludes the case of constant curves. There is also an example in [PV10] showing that, on certain constant curves, there can be points in $C(\mathbb{A}_k) \cap \overline{J(k)}$ which are not in $C(k)$ (though they are in $\overline{C(k)}$). Additionally, if $J(k)$ is finite, then the Brauer-Manin obstruction is the only obstruction to the Hasse principle, as shown by Scharaschkin [Sch99] for number fields, and the same argument applies to function fields. The above theorem, in the case of constant curves over function fields, extends these results of [Sch99, PV10] to cover some cases where the Jacobian is not simple.*

Proof. By the Weil bounds, C has a 0-cycle of degree 1. We may therefore view C as a subvariety of J as in Section 2.2. The Zariski closure Z of $J(k)$ is a finite union of torsion translates of (base changes of) proper abelian subvarieties of J defined over a finite field, so $Z \cap C$ is a 0-dimensional scheme defined over a finite field. Therefore all points lying on this intersection are points of C that are torsion in $J(\overline{k})$ of order dividing some integer n . This, together with the assumption that $C(\mathbb{F}) = \emptyset$ already implies that $C(k) = \emptyset$.

We now prove that the Brauer-Manin set is empty. Recall that Tate and Milne have proved that the Tate-Shafarevich group of a constant abelian variety is finite. (See Tate [Tat64] and Milne [Mil75, Theorem 8.1]. The restriction that $p \neq 2$ in [Mil75] can be lifted thanks to [Ill79].) Therefore, by Remark 2.3, it suffices to show that $C(\mathbb{A}_k) \cap \overline{J(k)} = \emptyset$, where $\overline{J(k)}$ denotes the closure of $J(k) \subset J(\mathbb{A}_k)$ in the adelic topology. The adelic points on this intersection all have components in $Z \cap C$ so have order dividing n . So the points on this intersection belong to the torsion subgroup of $\overline{J(k)}$ but that is just the torsion on $J(k)$ itself by [PV10, Lemma 3.7]. But, as we've seen above, $C(k) = \emptyset$ and the claim follows. \square

3. d -PRIMARY OBSTRUCTIONS FOR INFINITELY MANY COPRIME d

In this section we show that it is possible for a curve of genus at least 2 over a global field to have d -primary Brauer-Manin obstructions for infinitely many coprime d . This is very different than the case of genus one curves where the only obstructions come from the I -primary subgroup, where I is the index of the curve (see [CV17, Theorem 1.2]). Our proof also yields a construction of a hyperelliptic curve C with an odd Brauer-Manin obstruction to the Hasse principle (see Section 3.1). Interestingly, the Albanese torsor Alb_X^1 of a hyperelliptic curve X can *never* have an odd Brauer-Manin obstruction to the Hasse principle [CV17, Cor. 4.3].

Theorem 3.1. *There exists a curve C/\mathbb{Q} such that $C(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ and $C(\mathbb{A}_{\mathbb{Q}})^{\text{Br } C^{[d^\infty]}} = \emptyset$ for an infinite set of pairwise coprime integers d .*

Proposition 3.2. *Let C be a curve of index a_1 over a global field k whose Jacobian J has rank 0. Let v be a finite place of good reduction for C , let $p = \text{char } \mathbb{F}_v$ and let $d := p \cdot \#J(\mathbb{F}_v)$. If $\text{III}(k, J)^{[d^\infty]}$ is finite and $C(\mathbb{A}_k)^{\text{Br}} = \emptyset$, then $C(\mathbb{A}_k)^{\text{Br } C^{[d^\infty]}} = \emptyset$.*

Proof of Proposition 3.2. Since the index of C is 1, we may fix an embedding $\iota: C \hookrightarrow J$. We will assume that $C(\mathbb{A}_k)^{\text{Br } C[d^\infty]} \neq \emptyset$ for otherwise the theorem trivially holds. Let $(P_v) \in C(\mathbb{A}_k)^{\text{Br } C[d^\infty]}$. Since $\text{III}(k, J)[d^\infty]$ is finite, Corollary 2.8 implies that for each $n \geq 1$ there exists a $Q_n \in J(k)$ such that $(\iota(P_v) - Q_n) \in d^n J(\mathbb{A}_k)$. Since $J(k)$ is finite, there is some $Q \in J(k)$ such that $Q = Q_n$ for infinitely many n . As n goes to ∞ , $d^n J(k_v)$ converges to 0 (by definition of d), so $\iota(P_v)$ converges to $Q \in J(k)$. Thus Q is in the image of ι , so $C(k)$ and $C(\mathbb{A}_k)^{\text{Br}}$ are nonempty. \square

Remark 3.3. *It would be very interesting to determine if the hypothesis in Proposition 3.2 that $J(k)$ is finite is necessary.*

Remark 3.4. *If the index I of C is greater than 1 and $\text{III}(k, J)$ is finite, then C has an I -primary Brauer-Manin obstruction to the existence of rational points. Indeed, if C is not locally soluble, then this holds trivially. If C is locally soluble, then for each i , $\text{Pic}^i(C) = \text{Pic}^i(\overline{C})^{G_k} = \text{Alb}_C^i(k)$. By [CV17, Cor. 4.3] we have that Alb_C^1 has an I -primary obstruction. Hence the same is true for C by functoriality of the Brauer-Manin pairing. Example 3.10 below shows that in this situation it is still possible that C has d -primary Brauer-Manin obstructions for integers relatively prime to I .*

Theorem 3.1 would follow from Proposition 3.2 once one knows the existence of infinitely many places of good reduction such that $(\text{char } \mathbb{F}_v) \cdot (\#J(\mathbb{F}_v))$ are pairwise coprime. We will instead use the following variant of Proposition 3.2, which allows us to rely on the weaker statement that there exists an elliptic curve E with infinitely many places of good reduction such that $\#E(\mathbb{F}_v)$ are pairwise coprime.

Proposition 3.5. *Suppose $\pi: C \rightarrow A$ is a finite morphism from the curve C to an abelian variety A such that $\text{III}(k, A)$ and $A(k)$ are both finite. If there exists a prime v_0 of good reduction for C and A such that $\pi(C(\mathbb{F}_{v_0})) \cap (A(k) \bmod v_0) = \emptyset$, then $C(\mathbb{A}_k)^{\text{Br } C[d^\infty]} = \emptyset$ where $d = \#A(\mathbb{F}_{v_0})$.*

Proof. Suppose $(P_v) \in C(\mathbb{A}_k)^{\text{Br } C[d^\infty]}$. Then $\pi(P_v) \in A(\mathbb{A}_k)^{\text{Br } A[d^\infty]}$ and so, by Corollary 2.2, we see that for any positive integer n there exists $Q_n \in A(k)$ and $(R_v^{(n)}) \in A(\mathbb{A}_k)$ such that $\pi(P_v) - Q_n = d^n (R_v^{(n)})$. Since $A(k)$ is finite, we may assume $Q_n = Q \in A(k)$ is constant. Since $d = \#A(\mathbb{F}_{v_0})$, we see that the reduction of P_{v_0} is an \mathbb{F}_{v_0} -point on C that maps to $Q \bmod v_0$, resulting in a contradiction. \square

Lemma 3.6. *Let E be an elliptic curve over a global field k of characteristic not 2 with $E(k) = \{O\}$, let $\phi: E \rightarrow \mathbb{P}^1 = \mathbb{P}^1_{(x:z)}$ be a map given by $|2O|$ that sends O to ∞ , and let S be a finite set of places. If $q \in k$ is a sufficiently large, totally positive, principal prime that is congruent to 1 modulo $8\mathcal{O}_k$, then there exists a nice curve C/k admitting a double cover $\pi: C \rightarrow E$ such that*

- (1) π is branched over the points $\phi^*(V(x^2 - qz^2))$ and unramified at all other points,
- (2) $C(\mathbb{A}_k) \neq \emptyset$, and
- (3) $\mathbf{k}(\pi^{-1}(O))$ is equal to $k(\sqrt{p})$ for some totally positive principal prime p congruent to 1 modulo $8\mathcal{O}_k$ with $p \notin S$.

In particular, the set of places $v_0 \in \Omega_k$ such that the hypotheses of Proposition 3.5 hold has Dirichlet density $1/2$.

Remark 3.7. *In the case that k is a global function field, the conditions that q is totally positive and $q \equiv 1 \pmod{8\mathcal{O}_k}$ hold trivially. Indeed, the positivity condition vacuously holds since there are no archimedean places and 8 is either a unit or 0.*

Proof. A double cover $\pi: C \rightarrow E$ is determined, up to quadratic twist, by its branch locus. Let $\pi: C \rightarrow E$ be a double cover of E branched over $\phi^*(V(x^2 - qz^2))$ with the fiber above O split. For any $a \in k^\times/k^{\times 2}$, let $\pi^a: C^a \rightarrow E$ be the associated twist.

By Riemann-Hurwitz, C^a has genus 3. Thus, by Hensel's Lemma and the Hasse-Weil bounds, $C^a(k_v) \neq \emptyset$ for all finite v with $\#\mathbb{F}_v \geq 37$ and such that $(C^a)_{\mathbb{F}_v}$ is geometrically irreducible. Recall that a double cover is geometrically reducible if and only if the base is geometrically reducible or the divisor defining the double cover (in the case of π , this is $\phi^*(V(x^2 - qz^2)) - 4O$) is twice a principal divisor. Therefore, the places v where $(C^a)_{\mathbb{F}_v}$ is geometrically reducible are the places v such that $E_{\mathbb{F}_v}$ is geometrically reducible, the places that ramify in $k(\sqrt{q})$, and the places that ramify in $k(\sqrt{a})$.

Let p be a principal prime that is totally positive and congruent to 1 modulo $8\mathcal{O}_k$, that is a square modulo all places v with $\#\mathbb{F}_v \leq 37$, that is a square modulo all places v where $E \bmod v$ is geometrically reducible, that splits completely in $\mathbf{k}(\phi^*(V(x^2 - qz^2)))$, and that is not in S . Such a p exists, because all but the last condition can be imposed by asking that p split in a particular field extension, so Chebotarev's density theorem says that there are in fact infinitely many such p .

It is clear from the construction that C^p satisfies conditions (1) and (3). We claim that for such p , we also have $C^p(\mathbb{A}_k) \neq \emptyset$. As explained above, it suffices to check $C^p(k_v) \neq \emptyset$ for (i) $v \mid \infty$, (ii) v with $\#\mathbb{F}_v \leq 37$, (iii) v where $E_{\mathbb{F}_v}$ is geometrically reducible, (iv) places v that ramify in $k(\sqrt{q})$ and (v) places that ramify in $k(\sqrt{p})$. Since p is a square for all places of type (i), (ii) or (iii) and $C(\mathbb{A}_k) \neq \emptyset$ (in fact, $C(k) \neq \emptyset$), $C^p(k_v) \neq \emptyset$ for places of this type. Since q and p are totally positive principal primes that are congruent to 1 mod $8\mathcal{O}_k$, the only places that ramify in $k(\sqrt{q})$ and $k(\sqrt{p})$ are v_q and v_p . Since v_p splits completely in $\mathbf{k}(\phi^*(V(x^2 - qz^2)))$, there is a k_{v_p} -point in the branch locus of π^a for any twist $a \in k^\times/k^{\times 2}$ and hence a k_{v_p} -point on C^p . Furthermore, since q is a square modulo p and q and p are both totally positive primes and 1 modulo $8\mathcal{O}_k$, the product formula applied to the Hilbert symbol (q, p) implies that p is a square modulo q , so we also have that $C^p(k_{v_q}) \neq \emptyset$. Hence, $C^p(\mathbb{A}_k) \neq \emptyset$ as desired. \square

Proof of Theorem 3.1. Let E/\mathbb{Q} be an elliptic curve with $E(\mathbb{Q})$ trivial, $\text{III}(\mathbb{Q}, E)$ finite and $\text{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{F}_q)$ for every prime q . For example, one may take the curve with minimal Weierstrass equation $y^2 + y = x^3 + x^2 - 12x - 21$, [LMFDB, Elliptic Curve 67.a1].

By Serre's open image theorem [Ser72], there is a finite set of primes S such that for all $q \notin S$, $\mathbb{Q}(E[q])$ is linearly disjoint from $\mathbb{Q}(E[n])$ for any integer n with $q \nmid n$. Let $\pi: C \rightarrow E$ be a locally soluble double cover given by Lemma 3.6. Let $L = \mathbb{Q}(\sqrt{p})$ be the quadratic extension of \mathbb{Q} given by the residue field of $\pi^{-1}(O)$. By Lemma 3.6, p is a positive prime outside S that is congruent to 1 modulo 8. By Proposition 3.5 $C(\mathbb{A}_{\mathbb{Q}})^{\text{Br } C^{[d^\infty]}} = \emptyset$ for $d = \#E(\mathbb{F}_v)$ where v is any finite place in the set

$$T := \{v \in \Omega_{\mathbb{Q}} : E_{\mathbb{F}_v} \text{ smooth, and } O \notin \pi(C(\mathbb{F}_v))\}.$$

We will inductively construct a sequence of primes in T such that the corresponding integers $\#E(\mathbb{F}_v)$ are pairwise coprime. Since $p \equiv 1 \pmod{8}$, L is contained in $\mathbb{Q}(\zeta_p)$ and hence $\mathbb{Q}(E[p])$. Assume that there exist $v_1, \dots, v_i \in T$ such that the integers $\#E(\mathbb{F}_{v_j})$ are pairwise

coprime and such that $p \nmid \#E(\mathbb{F}_{v_j})$ for all j . Note that this assumption is satisfied in the base case $i = 1$ by the Chebotarev density theorem, since $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{F}_p)$. Let n be the radical of the product $\prod_{j=1}^i \#E(\mathbb{F}_{v_i})$. By the definition of S and the assumption that $p \nmid n$, the pair of fields $\mathbb{Q}(E[n])$ and $\mathbb{Q}(E[p])$ are linearly disjoint. This also implies that $\mathbb{Q}(E[n])$ and L are linearly disjoint.

Since the Galois representations on $E[q]$ are surjective for all primes $q \mid n$, there exists some element $\sigma \in \text{Gal}(E[n]/E)$ that fixes no nontrivial point of $E[n]$. Furthermore, since $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{F}_p)$, there exists an element $\tau \in \text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ such that $\tau|_L$ is nontrivial and τ fixes no nontrivial point of $E[p]$. (It suffices that 1 is not an eigenvalue and that the determinant is not a square.) Thus, the Chebotarev density theorem applied to the compositum of $\mathbb{Q}(E[p])$ and $\mathbb{Q}(E[n])$ yields a finite place $v_{i+1} \in T$ (since v_{i+1} is inert in L) such that $\#E(\mathbb{F}_{v_{i+1}})$ is relatively prime to np . \square

Remarks 3.8.

- (1) We expect that most curves over arbitrary global fields satisfy the conclusions of Theorem 3.1. On the other hand, in the next section, we will show that this is not the case for every curve.
- (2) Over \mathbb{Q} one might even expect that we can take all d to be prime in Theorem 3.1 for suitable curves, which would follow, e.g., from a conjecture of Koblitz [Kob88] that there are many elliptic curves for which $\#E(\mathbb{F}_v)$ is prime infinitely often.
- (3) We can also obtain a very different example satisfying the conclusion of Theorem 3.1 by applying Lemma 3.6 to $E : y^2 = x^3 - x + 2$ over $k = \mathbb{F}_3(t)$. Then E is defined over \mathbb{F}_3 and $\#E(\mathbb{F}_3) = 1$. Given any integer $n > 1$, if $f = [\mathbb{F}_3(E[n]) : \mathbb{F}_3]$ and ℓ is a prime number such that $(\ell, f) = 1$, then $(\#E(\mathbb{F}_{3^\ell}), n) = 1$. So, by picking successively suitable n, ℓ, v we get a list of places inert in L with $\#E(\mathbb{F}_v)$ pairwise coprime.

3.1. A hyperelliptic curve with an odd order Brauer-Manin obstruction. We close this section with the following application of Proposition 3.5, which gives a curve C of index 2 with odd order Brauer-Manin obstructions. This is particularly interesting because $C \subset \text{Alb}_C^1$ and the Brauer-Manin obstruction on Alb_C^1 is completely captured by the 2-primary subgroup (cf. [CV17, Thm 1.2 and Cor. 4.5]).

Lemma 3.9. *Let C/k be a hyperelliptic curve over a global field k of characteristic not equal to 2 with affine model $y^2 = f(x)$. Suppose $\text{III}(k, J)$ is finite and $J(k) = \{O\}$ is trivial. For any prime v of good reduction for J such that $f(x)$ has no linear factor mod v we have $C(\mathbb{A}_k)^{\text{Br } C^{[d^\infty]}} = \emptyset$ where $d = \#J(\mathbb{F}_v)$.*

Proof. There is a map $\phi : \text{Alb}_C^1 \rightarrow \text{Alb}_C^0 = J$ defined by sending the class of a degree 1 zero-cycle z to the class of $2z - (\infty^+ + \infty^-)$, where ∞^\pm are the points at infinity on the affine model defining C . Let $\pi : C \rightarrow J$ be the composition of ϕ with the canonical map $C \rightarrow \text{Alb}_C^1$. The result follows from Proposition 3.5 applied to the map π , since the fiber above O is defined by $f(x) = 0$. \square

Example 3.10. *The hyperelliptic curve C/\mathbb{Q} defined by $y^2 = 7(x^6 + 2x^4 + x^2 + 2x + 2)$ has index 2, $C(\mathbb{A}_\mathbb{Q}) \neq \emptyset$, and $C(\mathbb{A}_\mathbb{Q})^{\text{Br } C^{[\ell^\infty]}} = \emptyset$ for $\ell = 3, 5, 7$ and possibly infinitely many other primes.*

Proof. To ease notation write $J^1 := \text{Alb}_C^1$. Using Magma one can perform a 2-descent on J to determine that $\text{Sel}^2(k, J) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. A further 2-descent on J^1 as described in [Cre13]

gives that $J^1(\mathbb{Q}) = \emptyset$ and $\text{III}(k, J)[2] \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. Since C is locally soluble, the fact that $J^1(\mathbb{Q}) = \emptyset$ proves that C has no 0-cycle of degree 1, so C has index 2. J has good reduction at $v = 3, 5$ and 17 where the orders of $J(\mathbb{F}_v)$ are 9, 25 and 343, respectively. This shows that $J(\mathbb{Q})$ is trivial. So Lemma 3.9 gives that there is a d -primary Brauer-Manin obstruction for every $d = \#J(\mathbb{F}_v)$ such that $f(x)$ has no linear factor modulo these primes. This applies to $v = 3, 5, 17$. \square

4. DEGREES DO NOT CAPTURE THE BRAUER-MANIN OBSTRUCTION ON CURVES

In this section we construct examples of pointless curves over global fields that have index 1 and such that there are primes ℓ such that ℓ -primary subgroup of the Brauer group does not obstruct the existence of rational points. For any ℓ , a curve of index 1 has projective embeddings of degree ℓ^m provided m is sufficiently large. So these examples show, in particular, that degrees do not capture the Brauer-Manin obstruction to the existence of rational points on curves in the sense of [CV17, Question 1.1].

Theorem 4.1. *There exists a genus 3 curve C/\mathbb{Q} with index 1 such that $C(\mathbb{A}_{\mathbb{Q}})^{(\text{Br } C)_{\text{odd}}} \neq \emptyset$ and $C(\mathbb{A}_{\mathbb{Q}})^{\text{Br } C[2]} = \emptyset$.*

Theorem 4.2. *For any prime number ℓ , there exists a global field k and a genus 2 curve C/k of index 1 such that $C(\mathbb{A}_k)^{\text{Br } C[\ell^\infty]} \neq \emptyset$ and $C(\mathbb{A}_k)^{\text{Br}} = \emptyset$.*

Remark 4.3. *In the case $\ell = 2$, this second example shows that even the canonical degree does not capture the Brauer-Manin obstruction to the existence of rational points on curves.*

Remark 4.4. *If $C(\mathbb{A}_k)^{\text{Br } C[\ell^\infty]} \neq \emptyset$, then by Corollary 2.5 there is, for every $n \geq 1$, an adelic point of C which lifts to an ℓ^n -covering of C . If $C(k) = \emptyset$, these coverings are counterexamples to the Hasse principle. For the curve C constructed in the proof of Theorem 4.1, the pullback of multiplication by any odd integer n on J (with no twisting) gives a covering which is a counterexample to the Hasse principle. Thus one has an infinite tower of non-isomorphic abelian étale coverings of C in which all covers are counterexamples to the Hasse principle.*

The idea behind these constructions is to find curves embedded in their Jacobians so that they contain, everywhere locally, nontrivial torsion points of order prime to ℓ . This gives adelic points that are ℓ^∞ -divisible, so by the results in Section 2.2 this gives points in $C(\mathbb{A}_k)^{\text{Br } C[\ell^\infty]}$. Section 4.1 contains the core of this idea and the proof of Theorem 4.1 and Section 4.2 focuses on the case of constant curves, which is used to prove Theorem 4.2 therein.

4.1. Adelic torsion packets. Let C be a nice curve over a global field k . Define an equivalence relation on $C(\bar{k})$ by declaring that $x \sim y$ if some multiple of the divisor $x - y$ is principal. The equivalence classes under this relation are called **torsion packets**. Let us say that a subset T of some torsion packet is an n -torsion packet if $n(t - s)$ is principal for all $t, s \in T$.

Proposition 4.5. *Suppose there is an n -torsion packet T on C and there is a zero-cycle of degree 1 supported on T . Then $T(\mathbb{A}_k) \subset C(\mathbb{A}_k)^{\text{Br } C[d^\infty]}$ for any d relatively prime to n .*

Proof. Let z be a 0-cycle of degree 1 supported on T and let $\iota : C \rightarrow J$ be the corresponding embedding given by $x \mapsto [x - z]$. For $t \in T(\bar{k})$, $\iota(t) = t - z$ is a sum of differences of pairs

$t_i - t_j$ with $t_i, t_j \in T(\bar{k})$. Each difference $t_i - t_j$ lies in $J[n]$ since T is an n -torsion packet. So $\iota(t) \in J[n]$. Thus, if $(Q_v) \in T(\mathbb{A}_k)$, then $\iota(Q_v) \in J(\mathbb{A}_k)[n] \subset d^\infty J(\mathbb{A}_k)$. Corollary 2.8 then shows that $(Q_v) \in C(\mathbb{A}_k)^{\text{Br } C[d^\infty]}$. \square

Proof of Theorem 4.1. Let T be the 0-dimensional subscheme of $\mathbb{A}_{\mathbb{Q}}^1$ that is given by the vanishing of $f(x) = (x^2 + 3)(x^3 - 19)$; note that T is a counterexample to the Hasse principle. For any square free polynomial $g(x) \in \mathbb{Q}[x]$ relatively prime to $f(x)$, the set of Weierstrass points of the hyperelliptic curve $C : y^2 = f(x)g(x)$ is a 2-torsion packet containing T and the support of a zero-cycle of degree 1. By Proposition 4.5 we have that $T(\mathbb{A}_{\mathbb{Q}}) \subset C(\mathbb{A}_{\mathbb{Q}})^{(\text{Br } C)_{\text{odd}}}$ and so $C(\mathbb{A}_{\mathbb{Q}})^{(\text{Br } C)_{\text{odd}}} \neq \emptyset$. It remains to show that $g(x)$ can be chosen so that $C(\mathbb{A}_{\mathbb{Q}})^{\text{Br } C[2]} = \emptyset$. For this one can take $g(x) = 2(x^3 + x + 1)$. A 2-descent (implemented in Magma based on [BS09]) shows that $C(\mathbb{Q}) = \emptyset$. Moreover, by Corollary 2.5, we have that the set $C(\mathbb{A}_{\mathbb{Q}})^{2\text{-ab}}$ of adelic points on C that survive a 2-descent is equal to set cut out by $\text{Br } C[2]$. Hence $C(\mathbb{A}_{\mathbb{Q}})^{(\text{Br } C)[2]} = \emptyset$ as desired. \square

4.2. Constant curves over function fields. For constant curves over global function fields the existence of local torsion points is guaranteed for all but finitely many primes. The following lemma ensures the existence of local torsion points of order prime to ℓ , for any prime ℓ .

Lemma 4.6. *Let C_0/\mathbb{F}_q be a curve of genus $g > 1$ embedded in its Jacobian J_0 . Let ℓ be a prime number and write $\#J_0(\mathbb{F}_{q^n}) = \ell^{r_n} m_n, \ell \nmid m_n$. If $q^n > (2g\ell^{r_n})^2$, then there exists a point in $C_0(\mathbb{F}_{q^n})$ of order prime to ℓ in J_0 . Moreover, the inequality $q^n > (2g\ell^{r_n})^2$ will hold for all n sufficiently large.*

Proof. For the first part of the theorem, it is enough to consider $n = 1, r = r_1$ and assume that $q > (2g\ell^r)^2$. There exists an abelian variety A/\mathbb{F}_q and a separable isogeny $\phi: A \rightarrow J_0$ of degree ℓ^r for which $\phi(A(\mathbb{F}_q))$ is the subgroup of $J_0(\mathbb{F}_q)$ of points of order prime to ℓ . To prove the lemma it is enough to show that the curve $\phi^*(C_0)$ has an \mathbb{F}_q -rational point. The genus g' of $\phi^*(C_0)$ satisfies $2g' - 2 = \ell^r(2g - 2)$ and the statement of the lemma now follows from the Weil bound applied to $\phi^*(C_0)$.

For the second part, recall that there exist algebraic integers $\alpha_1, \dots, \alpha_{2g}$ with $|\alpha_i| = q^{1/2}$, the eigenvalues of Frobenius, such that $\#J_0(\mathbb{F}_{q^n}) = \prod(\alpha_i^n - 1)$. As the α_i are not roots of unity, whenever they are ℓ -adic units, the multiplicative order of α_i modulo ℓ^r grows exponentially with r . Therefore the smallest n such that $\#J_0(\mathbb{F}_{q^n})$ is divisible by ℓ^r grows exponentially with r and so satisfies $q^n > (2g\ell^r)^2$ with finitely many exceptions. \square

Proposition 4.7. *Let C_0/\mathbb{F}_q and ℓ be as as in Lemma 4.6, and k/\mathbb{F}_q a function field in one variable such that for all $n \leq 2 \log_q(2g\ell^{r_n})$ (using the notation from Lemma 4.6), k has no places of degree n . Then the curve $C := C_0 \times_{\mathbb{F}_q} k$ satisfies $C(\mathbb{A}_k)^{\text{Br } C[\ell^\infty]} \neq \emptyset$.*

Remark 4.8. *By Lemma 4.6, there are only finitely many n such that $n \leq 2 \log_q(2g\ell^{r_n})$.*

Proof. Lemma 4.6 provides, for every place v of k , an infinitely ℓ -divisible point in C with coordinates in the residue field of v so, a fortiori, in the completion k_v . The adelic point with these points as coordinates belong to $C(\mathbb{A}_k)^{\text{Br } C[\ell^\infty]}$ by Corollary 2.8. \square

Proof of Theorem 4.2. Consider the curve $C_0 : y^2 = -x^6 + x^2 - 1$ over \mathbb{F}_3 and let k_m be the function field of the curve $D_m : (x^{3^m} - x + 1)(y^{3^m} - y - 1) = 1$ over \mathbb{F}_3 . It is easy to check

that $D_m(\mathbb{F}_{3^m})$ is empty. So for m sufficiently large, Proposition 4.7 applies to give that the curve $C := C_0 \times_{\mathbb{F}_3} k_m$ over k_m has $C(\mathbb{A}_{k_m})^{\text{Br} C[\ell^\infty]} \neq \emptyset$. The Jacobian J_0 of C_0 is isogenous to the product of two elliptic curves, one ordinary and other supersingular. Indeed, there is an obvious morphism to the supersingular elliptic curve given by $y^2 = -x^3 + x - 1$. The other factor is the curve $y^2 = -x^3 + x^2 - 1$, which is ordinary. By results of [Sub75] the Jacobian of D_m is ordinary. It follows that there can be no surjective map $D_m \rightarrow C_0$. But there is no constant map either because $C_0(\mathbb{F}_3) = \emptyset$. Hence $C(k_m)$ is empty. Moreover, any map $D_m \rightarrow J_0$ lands in a coset of the ordinary factor of J_0 . So, the k_m -rational points of $J = J_0 \times k$ are not Zariski dense and Theorem 2.14 gives that $C(\mathbb{A}_k)^{\text{Br}} = \emptyset$. \square

5. POONEN'S HEURISTIC

We remind the reader of the Poonen-Scharaschkin set $C(\mathbb{A}_k)^{\text{PS}}$ defined in Section 2.3. Poonen conjectured [Poo06, Conjecture 5.1] that a pointless curve C of genus at least 2 over a number field k has $C(\mathbb{A}_k)^{\text{PS}} = \emptyset$, or, equivalently, that there exist a finite set S of finite places of good reduction such that the images of $J(k)$ and $\prod_{v \in S} C(\mathbb{F}_v)$ in $\prod_{v \in S} J(\mathbb{F}_v)$ do not intersect. By Scharaschkin's result (cf. Remark 2.11), Poonen's conjecture implies that the Brauer-Manin obstruction is the only obstruction to the existence of rational points on curves over number fields. As evidence for the conjecture Poonen gives an analysis of the probability that the intersection is nonempty assuming:

- (1) the numbers $\#J(\mathbb{F}_v)$ are at least as smooth as typical integers of the same size, and
- (2) the subsets $\iota(C(\mathbb{F}_v)) \subset J(\mathbb{F}_v)$ are modeled on random subsets of the same size, independent of v .

Specifically, Poonen makes the following conjecture and derives the following consequence.

Conjecture 5.1 ([Poo06, Conj. 7.1]). *Let A be an abelian variety over a number field k with S_A the set of primes of good reduction for A , and let $u \in (0, 1)$. Then*

$$\limsup_{B \rightarrow \infty} \frac{\#\{v \in S_A : \#\mathbb{F}_v \leq B \text{ and } \#A(\mathbb{F}_v) \text{ is } B^u \text{ smooth}\}}{\#\{v \in S_A : \#\mathbb{F}_v \leq B\}} > 0.$$

Theorem 5.2 ([Poo06, Thm. 7.2]). *Let C be a curve of genus at least 2 over a number field k with Jacobian J and let S_C be the set of primes of good reductions for C . Assume Conjecture 5.1 holds for J . For each prime $v \in S_C$, let \mathcal{C}_v be a random subset of $J(\mathbb{F}_v)$ of size $\#C(\mathbb{F}_v)$; assume that the choices for different v are independent. Then with probability 1, there exists a finite subset $S \subset S_C$ such that the images of $J(k)$ and $\prod_{v \in S} \mathcal{C}_v$ in $\prod_{v \in S} J(\mathbb{F}_v)$ do not intersect.*

In this section we show that the same assumptions and analysis lead to the expectation that a pointless curve C over a number field of genus at least 2 has $C(\mathbb{A}_k)^{\text{PS}[d^\pm]} = \emptyset$, for any integer d (See Theorem 5.3 below). However, the curve C/\mathbb{Q} produced by Theorem 4.1 provides a counterexample to this statement. Indeed, it has $C(\mathbb{Q}) = C(\mathbb{A}_\mathbb{Q})^{\text{Br}} = \emptyset$, but $C(\mathbb{A}_\mathbb{Q})^{\text{Br} C[2^\pm]} \neq \emptyset$. Proposition 2.10 then implies that $C(\mathbb{A}_\mathbb{Q})^{\text{PS}[2^\pm]} \neq \emptyset$.

It is fairly easy to see where the heuristic goes astray in this example. The curve has the property that $\iota(C(\mathbb{A}_\mathbb{Q}))$ contains elements of $J(\mathbb{A}_\mathbb{Q})[2]$, implying that the subsets $\iota(C(\mathbb{F}_v)) \subset J(\mathbb{F}_v)$ all contain 2-torsion points of $J(\mathbb{F}_v)$. This illustrates an important point that these subsets cannot be modeled by random subsets of the appropriate size even when C has no rational points.

Theorem 5.3. *Let C be a curve of genus at least 2 over a number field k with Jacobian J , let S_C be the set of primes of good reductions for C , and let $d \geq 1$ be an integer. Assume Conjecture 5.1 holds for J . For each prime $v \in S_C$, let C_v be a random subset of $J(\mathbb{F}_v)[d^\perp]$ of size $\#C(\mathbb{F}_v)$; assume that the choices for different v are independent. Then with probability 1, there exists a finite subset $S \subset S_C$ such that the images of $J(k)$ and $\prod_{v \in S} C_v$ in $\prod_{v \in S} J(\mathbb{F}_v)[d^\perp]$ do not intersect.*

Proof. Our proof of this theorem follows Poonen’s argument proving Theorem 5.2. Let G be a finitely generated abelian group, S a positive density set of finite places of k , $\{G_v\}_{v \in S}$ a collection of finite abelian groups with homomorphisms $G \rightarrow G_v$, and $\{C_v\}_{v \in S}$ a collection of random finite subsets where the choices for different v are independent. Poonen’s argument shows that if $\#C_v = O(\#\mathbb{F}_v)$, $\#G_v = (\#\mathbb{F}_v)^{g+o(1)}$ for some real number $g > 1$ that is independent of v , and each $\#G_v$ is b -smooth where $b = \sqrt{\#\mathbb{F}_v}$, then with probability 1 there exists a finite subset $S' \subset S$ such that the images of G and $\prod_{v \in S'} C_v$ in $\prod_{v \in S'} G_v$ do not intersect.

We will apply this with $G = J(k)$ and $G_v = J(\mathbb{F}_v)[d^\perp]$. Conjecture 5.1 implies that there is a positive density set S_1 of primes such that $J(\mathbb{F}_v)[d^\perp]$ is b -smooth for $b = \sqrt{\#\mathbb{F}_v}$. By the Weil conjectures $\#J(\mathbb{F}_v)[d^\perp] \cdot \#J(\mathbb{F}_v)[d^\infty] = \#J(\mathbb{F}_v) = (\#\mathbb{F}_v)^{g+o(1)}$. Let S_N denote the set of places such that $\#J(\mathbb{F}_v)[d^\infty] \geq N$. These sets have, by Chebotarev’s density theorem, natural densities which we claim tend to 0 as N tends to ∞ . It follows that there are sets of primes of density arbitrarily close to 1 on which $J(\mathbb{F}_v)[d^\infty]$ is bounded. Hence there is a positive density set of places $S_2 \subset S_1$ such that $\#J(\mathbb{F}_v)[d^\perp] = (\#\mathbb{F}_v)^{g+o(1)}$ as required. Thus the proof of the claim follows from the following lemma, after observing that for each integer d and each $v \nmid d$, the reduction map gives a surjective map $J(k_v)[d^\infty] \rightarrow J(\mathbb{F}_v)[d^\infty]$. \square

Lemma 5.4. *Let A be an abelian variety over a number field k . The density of the set of places v of k such that $A(k_v)$ has a point of order ℓ^n tends to 0 as n tends to ∞ .*

Proof. Let $G_n \subset \mathrm{GSp}_{2 \dim(A)}(\mathbb{Z}/\ell^n)$ denote the image of the representation of $\mathrm{Gal}(k)$ on $A[\ell^n]$ in some fixed basis, and let $G_{n,1} \subset G_n$ denote the subset of matrices with 1 as an eigenvalue. The density of the set of places such that $A(k_v)$ has a point of order ℓ^n is equal to $\#G_{n,1}/\#G_n$ by Chebotarev’s density theorem. By a result of Serre in [Ser79] (see also [McQ95, Corollary 2.1.7]), there is an integer m , depending on A but independent of n , such that G_n contains $(\mathbb{Z}/\ell^n)^{\times m}$ as a subgroup of scalar matrices. Therefore we have a map of sets $(\mathbb{Z}/\ell^n)^{\times m} \times G_{n,1} \rightarrow G_n$ sending (λ, M) to λM . If $N = \lambda M$ is in the image of this map, then λ is an eigenvalue of N . Hence the preimage of N has size at most $2 \dim(A)$, which is independent of n . On the other hand, $\#(\mathbb{Z}/\ell^n)^{\times m}$ is unbounded as n goes to infinity, so $\#G_{n,1}/\#G_n \rightarrow 0$ as $n \rightarrow \infty$. \square

REFERENCES

- [BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. [↑12](#)
- [Čes15] Kęstutis Česnavičius, *Poitou-Tate without restrictions on the order*, Math. Res. Lett. **22** (2015), no. 6, 1621–1666. [↑4](#)
- [Cre13] Brendan Creutz, *Explicit descent in the Picard group of a cyclic cover of the projective line*, Algorithmic number theory: Proceedings of the 10th Biennial International Symposium (ANTS-X) held in San Diego, July 9–13, 2012 (Everett W. Howe and Kiran S. Kedlaya, eds.), Open Book Series, vol. 1, Mathematical Science Publishers, 2013, pp. 295–315. [↑10](#)

- [CV17] Brendan Creutz and Bianca Viray, *Degree and the Brauer-Manin obstruction (with an appendix by Alexei N. Skorobogatov)* (2017), available at [arXiv:1703.02187v2](https://arxiv.org/abs/1703.02187v2). (preprint). [↑1](#), [2](#), [7](#), [8](#), [10](#), [11](#)
- [Cor07] Patrick Corn, *The Brauer-Manin obstruction on del Pezzo surfaces of degree 2*, Proc. Lond. Math. Soc. (3) **95** (2007), no. 3, 735–777. [↑2](#)
- [Ill79] Luc Illusie, *Complexe de de Rham-Witt et cohomologie cristalline*, Ann. Sci. École Norm. Sup. (4) **12** (1979), no. 4, 501–661. [↑7](#)
- [Kob88] Neal Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165. [↑10](#)
- [LMFDB] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2017. [Online; accessed 16 October 2017]. [↑9](#)
- [Man71] Yuri I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Gauthier-Villars, Paris, 1971, pp. 401–411. [↑1](#), [2](#)
- [Mil75] James S. Milne, *On a conjecture of Artin and Tate*, Annals of Mathematics. Second Series **102** (1975), no. 3, 517–533. [↑7](#)
- [Mil80] ———, *Étale Cohomology*, Princeton Univ. Press, 1980. [↑3](#)
- [Mil06] ———, *Arithmetic Duality Theorems*, Second edition, BookSurge, LLC, 2006. [↑4](#)
- [McQ95] Michael McQuillan, *Division points on semi-abelian varieties*, Invent. Math. **120** (1995), no. 1, 143–159. [↑14](#)
- [Nak17] Masahiro Nakahara, *Brauer classes that never obstruct the Hasse principle for genus 1 fibrations* (2017), available at [arXiv:1706.07019v2](https://arxiv.org/abs/1706.07019v2). preprint. [↑2](#)
- [NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. [↑3](#)
- [Poo06] Bjorn Poonen, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. [↑1](#), [2](#), [13](#)
- [PV10] Bjorn Poonen and José Felipe Voloch, *The Brauer-Manin obstruction for subvarieties of abelian varieties over function fields*, Ann. of Math. (2) **171** (2010), no. 1, 511–532. [↑1](#), [2](#), [4](#), [7](#)
- [Roy88] H. L. Royden, *Real analysis*, 3rd ed., Macmillan Publishing Company, New York, 1988. [↑6](#)
- [Sch99] Victor Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, 1999. Ph.D. thesis, University of Michigan. [↑5](#), [6](#), [7](#)
- [Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (French). [↑9](#)
- [Ser79] ———, *Quelques propriétés des groupes algébriques commutatifs*, Astérisque (1979), 69–70. [↑14](#)
- [Sko01] Alexei N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. [↑1](#), [3](#), [4](#)
- [SZ16] Alexei N. Skorobogatov and Yuri G. Zarhin, *Kummer varieties and their Brauer groups* (2016), available at [arXiv:1612.05993](https://arxiv.org/abs/1612.05993). 24 pages, preprint. [↑2](#)
- [Sto07] Michael Stoll, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391. [↑1](#), [3](#), [4](#)
- [Sub75] Doré Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), no. 2, 169–193. [↑13](#)
- [SD93] Peter Swinnerton-Dyer, *The Brauer group of cubic surfaces*, Math. Proc. Cambridge Philos. Soc. **113** (1993), no. 3, 449–460. [↑2](#)
- [Tat64] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog* (1964), 415–440. Séminaire Bourbaki. Vol. 9, Exp. No. 306. [↑7](#)

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CANTERBURY, PRIVATE BAG 4800,
CHRISTCHURCH 8140, NEW ZEALAND

E-mail address: brendan.creutz@canterbury.ac.nz

URL: <http://www.math.canterbury.ac.nz/~b.creutz>

UNIVERSITY OF WASHINGTON, DEPARTMENT OF MATHEMATICS, BOX 354350, SEATTLE, WA 98195,
USA

E-mail address: bviray@math.washington.edu

URL: <http://math.washington.edu/~bviray>

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CANTERBURY, PRIVATE BAG 4800,
CHRISTCHURCH 8140, NEW ZEALAND

E-mail address: felipe.voloch@canterbury.ac.nz

URL: <http://www.math.canterbury.ac.nz/~f.voloch>