BRAUER-MANIN OBSTRUCTIONS ON HYPERELLIPTIC CURVES

BRENDAN CREUTZ AND DUTTATREY NATH SRIVASTAVA

Abstract. We describe a practical algorithm for computing Brauer-Manin obstructions to the existence of rational points on hyperelliptic curves defined over number fields. This offers advantages over descent based methods in that its correctness does not rely on rigorous class and unit group computations of large degree number fields. We report on experiments showing it to be a very effective tool for deciding existence of rational points: Among a random samples of curves over $\mathbb{Q}$ of genus at least 5 we were able to decide existence of rational points for over 99% of curves. We also demonstrate its effectiveness for high genus curves, giving an example of a genus 50 hyperelliptic curve with a Brauer-Manin obstrution to the Hasse Principle. The main theoretical development allowing for this algorithm is an extension of the descent theory for abelian torsors to a framework of torsors with restricted ramification.

1. Introduction

This paper is concerned with the problem of deciding the existence of a rational point on a algebraic curve C defined over a number field k. For curves of genus 0 it has long been known that the existence of k-rational points is decidable, as it is equivalent to the existence of points defined over the local fields containing k. For curves of positive genus the local-global principle can fail and there is no proven algorithm to decide if the set $C(k)$ of k-rational points is nonempty. However, it has been conjectured that the nonexistence of rational points on curves can always be explained by a Brauer-Manin obstruction [Poo06, Sto07] (This was first posed as a question in [Sko01]). If the conjecture is true, then the existence of rational points on curves is decidable because searching for points by day and searching for obstructions by night must eventually produce an answer.

We describe a practical algorithm to compute the obstruction coming from the elements of order 2 in the Brauer group of a hyperelliptic curve. We have implemented the algorithm in the Magma computational algebra system [BCP97] and find it performs well for hyperelliptic curves of genus $g \leq 10$ given by equations with moderately sized coefficients. We also find that it is a very effective tool for deciding existence of rational points. In a sample of genus 5 curves over $\mathbb{Q}$ drawn by choosing the coefficients of a defining polynomial uniformly at random from integers of size ≤ 100, the algorithm demonstrated a (nonlocal) Brauer-Manin obstruction for over two thirds of the curves, enabling us to decide on the existence of points for 99.6% of the curves considered. For curves of genus 10 with coefficients of size absolutely bounded by 10, we were able to decide existence of rational points for all of the curves in our sample. Such a level of success is in line with the recent result of Bhargava [Bha13] that a density approaching 100% of hyperelliptic curves of genus g have an obstruction coming from the 2-torsion subgroup $\mathrm{Br}(C)[2]$ of the Brauer group of the curve (or a local obstruction).

Our approach requires that we can identify and explicitly represent the correct elements in the infinite group $\mathrm{Br}(C)[2]$ to be used in the computation, and herein lies the main

theoretical novelty of the paper. In Section 3 we extend the descent theory for torsors under finite abelian group schemes described in [Sko01, Chapter 6] building on [CTS87] to handle torsors unramified outside a given set of places S of the number field (the original case being when S consists of all places). This enables us to prove that the obstruction coming from $\mathrm{Br}(C)[2]$ is equivalent to that coming from the 'unramified outside S subgroup' of $\mathrm{Br}(C)[2]$ for a finite set S (See Theorem 3.1 for the precise statement, which applies more generally to any smooth projective and geometrically integral variety). We believe this development will be of interest in its own right. Its relevance in the present context is that it allows us to bound the running time of our algorithm a priori because (modulo constant algebras) the unramified outside S subgroup is finite.

To write down explicit elements of $\mathrm{Br}(C)[2]$ that are unramified outside S, we make use of [CV15], which gives an explicit construction of Brauer classes in a certain subgroup which we denote by $\mathrm{Br}_\Upsilon(C)[2] \subset \mathrm{Br}(C)[2]$. In Section 4 we show, somewhat surprisingly, that the obstruction coming from $\mathrm{Br}(C)[2]$ is equivalent to that coming from $\mathrm{Br}_\Upsilon(C)[2]$. The proof of this fact relies on an interpretation of the elements of the fake Selmer set in [BS09] in terms of torsors that are not geometrically connected. While the result here is specific to the situation of hyperelliptic curves, the idea may prove useful in understanding the connection between Brauer-Manin obstructions and the 'fake descents' described in [PS97, BPS16, Cre20] and elsewhere.

1.1. **Comparison with other methods.** It is known that the obstruction coming from $\mathrm{Br}(C)[2]$ is equivalent to the two-cover descent obstruction described in detail in [BS09] building on [BF05]. Building on this, our approach offers significant advantages. To explain, let us compare the methods. The descent algorithm first computes a finite set of two-coverings with the property that it contains all locally solvable coverings and then carries out local computations to find the subset of them that are actually locally solvable. The result is a partition of the set of adelic points surviving 2-descent in the form

$$C(k) \subset C(\mathbb{A}_k)^{2\text{-desc}} = \bigcup_{(Y,\pi)\in \mathrm{Sel}^2(C/k)} \pi(Y(\mathbb{A}_k))\,.$$

The first step requires class and unit group information in number fields of degree $O(g)$. While there are subexponential algorithms whose correctness is conditional on the generalized Riemann hypothesis, rigorous computation is usually infeasible for $g > 1$. If this is not computed rigorously, then there is no guarantee that the resulting set contains all of the k-rational points.

By way of contrast, the set of adelic points orthogonal to a subgroup $B \subset \mathrm{Br}(C)$ is an intersection ,

$$C(k) \subset C(\mathbb{A}_k)^B = \bigcap_{\mathcal{A}\in B} C(\mathbb{A}_k)^{\mathcal{A}}\,,$$

where $C(\mathbb{A}_k)^{\mathcal{A}}$ is the set of adelic points that are orthogonal to $\mathcal{A}$. To compute this one enumerates the elements $\mathcal{A}_1, \mathcal{A}_2, \ldots$ of B and at the nth step computes the intersection of the first n. At every step of the process one has a set $X_n = C(\mathbb{A}_k)^{\{\mathcal{A}_1,\ldots,\mathcal{A}_n\}}$ which is guaranteed (unconditionally) to contain $C(k)$. This allows us to give an algorithm with similar complexity to the conditional descent algorithm, but whose output is rigorous (See Theorem 4.4 and Algorithm 5.1). Moreover, there are situations in which even the conditional descent algorithm is infeasible but we are able to produce a Brauer class and check that it

gives an obstruction. In Proposition 6.2 we give an example of a genus 50 hyperelliptic curve over $\mathbb{Q}$ with a Brauer-Manin obstruction to the local-global principle. Using the algorithm of [BS09] this would require class and unit group computations in a number field of degree 102 which is completely infeasible even assuming GRH.

There are other methods for computing the set of rational points on general curves including p-adic methods based on ideas of Chabauty [Cha41] (See [Poo21] for recent developments in this direction) as well as the Mordell-Weil Sieve [Sch99, Fly04, BS10]. These require an explicit embedding of the curve in its Jacobian given either by a rational point (in which case existence of points is already decided) or by a rational divisor of degree 1. Deciding existence of such an embedding is equivalent to deciding existence of rational points on the torsor Pic^1_C parameterizing divisor classes of degree 1 on C. In practice this can be approached using descent algorithms as described in [Cre13] or [CV15, Section 6] or via the Brauer-Manin obstruction using the techniques developed in this paper, with the latter having advantages over the former similar to those described above in the context of points on curves. It should also be noted that these methods require knowledge the set of rational points on the Jacobian, which typically requires the use of descent based techniques relying on GRH for their practical implementation.

1.2. **Outline of the paper.** Section 2 sets some notation and definitions used throughout the paper. Sections 3 and 4 are, as noted above, devoted to developing the required connections between the descent and Brauer-Manin obstructions to enable the algorithm. Section 4 also recalls the explicit description of Brauer classes given in [CV15] and provides some further details regarding the evaluation of these Brauer classes at points on the curve. Details of the algorithm are given in Section 5. In Section 6 we provide the results of experiments with the algorithm as well as some specific examples.

1.3. **Acknowledgements.** Both authors were supported by the Marsden Fund Council administered by the Royal Society of New Zealand. The first author thanks Bianca Viray for initial discussions on the possibility of using the results of [CV15] to compute Brauer-Manin obstructions along the lines described here.

2. Notation

Throughout the paper k will denote a field of characteristic 0. When k is a number field we use Ω_k to denote the set of places of k, $S \subset \Omega_k$ to denote a subset containing all archimedean primes and $\mathcal{O}_{k,S} \subset k$ to denote the ring of S-integers. Given $v \in \Omega_k$ we use k_v to denote the completion of k at v and $\mathcal{O}_v$ to denote the ring of integers in k_v.

Let M be a finite étale abelian k-group scheme whose order is a unit in $\mathrm{Spec}(\mathcal{O}_{k,S})$. Given $v \in \Omega_k$ we say that an element $\xi \in \mathrm{H}^1(k_v, M)$ (or in $\mathrm{H}^1(k, M)$) is unramified (at v) if it lies in the kernel of the restriction map to $\mathrm{H}^1(k_v^{\mathrm{unr}}, M)$, where k_v^{unr} is the maximal unramified extension of k_v. For any $v \in \Omega_k$, the cup product induces a canonical nondegenerate pairing [Mil06, Corollary I.2.3]

$$\mathrm{H}^1(k_v, M) \times \mathrm{H}^1(k_v, M^\vee) \to \mathbb{Q}/\mathbb{Z}\,, \tag{2.1}$$

where $M^\vee = \mathrm{Hom}_k(M, \mathbb{G}_m)$ is the Cartier dual of M. If $M(k_v^{\mathrm{unr}}) = M(\overline{k})$, then the unramified subgroups are exact annihilators by [Mil06, Theorem I.2.6]. In general, the exact

annihilator of the unramified subgroup of $\mathrm{H}^1(k_v, M^\vee)$ may be larger than the unramified subgroup of $\mathrm{H}^1(k_v, M)$.

We define $\mathrm{H}^1_S(k, M)$ to be the subgroup of elements of $\mathrm{H}^1(k, M)$ that are orthogonal to the unramified subgroup of $\mathrm{H}^1(k_v, M^\vee)$ for all $v \notin S$. When M spreads out to a smooth group scheme $\mathcal{M}$ over $\mathrm{Spec}(\mathcal{O}_{k,S})$, then $\mathrm{H}^1_S(k, M)$ consists of those elements that are unramified outside S and $\mathrm{H}^1_S(k, M)$ can be identified with the étale cohomology group $\mathrm{H}^1(\mathcal{O}_{k,S}, \mathcal{M})$ (see [Mil06, Proposition II.2.9] and [Poo17, Section 6.5.7]). We define

$$Ш^i_S(k, M) := \ker\left(\mathrm{H}^i_S(k, M) \to \prod_{v\in S} \mathrm{H}^i(k_v, M)\right).$$

When $S = \Omega_k$ we abbreviate $Ш^i(k, M) := Ш^i_{\Omega_k}(k, M)$. When M spreads out to a smooth group scheme over $\mathrm{Spec}(\mathcal{O}_{k,S})$, our $Ш^1_S(k, M)$ agrees with that of [Mil06, Theorem I.4.10], from which it follows that $Ш^1_S(k, M)$ is finite for any S. Indeed, we can enlarge S to S' so that M spreads out and use that $Ш^1_S(k, M) \subset Ш^1_{S'}(k, M)$.

The Brauer group of a scheme X is defined as the étale cohomology group $\mathrm{Br}(X) := \mathrm{H}^2(X, \mathbb{G}_m)$. When X is a variety over a field k, we use $\mathrm{Br}_0(X)$ to denote the image of the natural map $\mathrm{Br}(k) \to \mathrm{Br}(X)$ and $\mathrm{Br}_1(X)$ to denote the kernel of the natural map $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})$, where $\overline{X} = X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$ is the base change of X to an algebraic closure of k. For a commutative ring R we define $\mathrm{Br}(R) := \mathrm{H}^2(\mathrm{Spec}(R), \mathbb{G}_m)$.

3. A computable description of the Brauer-Manin obstruction

Throughout this section k will denote a number field. Suppose X is a smooth, projective and geometrically integral variety over k, G is a finite étale abelian group scheme over k and $M = G^\vee := \mathrm{Hom}(G, \mathbb{G}_m)$. Let $\lambda : M(\overline{k}) \to \mathrm{Pic}(\overline{X})$ be a morphism of Galois modules. We consider X-torsors under G of type λ. For example, if X is a hyperelliptic curve with Jacobian J and $\lambda : J[2](\overline{k}) = \mathrm{Pic}^0(\overline{X})[2] \subset \mathrm{Pic}(\overline{X})$ is the inclusion map, then X-torsors of type λ are the two-coverings considered in [BS09]. For the precise definition see [Sko01, Definition 2.3.2].

Let $r : \mathrm{Br}_1(X) \to \mathrm{H}^1(k, \mathrm{Pic}(\overline{X}))$ be the canonical map from the Hochshild-Serre spectral sequence $\mathrm{H}^p(k, \mathrm{H}^q(\overline{X}, \mathbb{G}_m)) \Rightarrow \mathrm{H}^{p+q}(X, \mathbb{G}_m)$ [Sko01, (2.23)]. Then any subgroup $H \subset \mathrm{H}^1(k, M)$ gives rise to the subgroup $r^{-1}(\lambda_*(H)) \subset \mathrm{Br}_1(X)$. In particular, for any $S \subset \Omega_k$ containing all archimedean primes, the subgroups $Ш^1_S(k, M) \subset \mathrm{H}^1_S(k, M) \subset \mathrm{H}^1(k, M)$ defined in Section 2 determine subgroups

$$Б_{\lambda,S}(X) \subset \mathrm{Br}_{\lambda,S}(X) \subset \mathrm{Br}_\lambda(X) \subset \mathrm{Br}_1(X).$$

We note that $\mathrm{Br}_{\lambda,S}(X)/\mathrm{Br}_0(X)$ is finite when S is finite by [Mil06, Corollary I.4.15]. The following theorem gives a computable description of the obstruction coming from the infinite group $\mathrm{Br}_\lambda(X)/\mathrm{Br}_0(X)$.

Theorem 3.1. *Given X and λ there is an explicitly computable finite set of primes $S = S(X, \lambda)$ such that the images of $X(\mathbb{A}_k)^{\mathrm{Br}_\lambda(X)}$ and $X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)}$ in $\prod_{v\in S} X(k_v)$ coincide. In particular,*

$$X(\mathbb{A}_k)^{\mathrm{Br}_\lambda(X)} = \emptyset \quad \Leftrightarrow \quad X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)} = \emptyset.$$

The proof will be completed at the end of this section. It shows that we may take S to be any subset of Ω_k containing all archimedean primes such that X spreads out to a smooth

proper scheme over $\mathrm{Spec}(\mathcal{O}_{k,S})$, λ spreads out to a morphism of smooth proper group schemes and S contains

- all primes of residue cardinality below an explicit bound coming from the generalized Weil conjectures (which depends only on the Betti numbers in the cohomology of $\overline{Y} = Y \times_k \overline{k}$ where Y is a torsor of type λ), and
- enough primes to ensure a certain technical hypothesis holds in the case that λ is not injective (in which case the torsors of type λ are not geometrically connected).

The set just described is not the minimal S for which the theorem holds. We have taken care to state and prove the lemmas used in the proof for sets S smaller than that above where possible, even though this introduces a number of fairly technical points that could otherwise be avoided. Our reason for doing so is that we are ultimately interested in practical computations, in which case it is best to take S as small as possible. These lemmas will be used also in the proof of Theorem 4.4, which is a version of Theorem 3.1 for hyperelliptic curves allowing S to omit odd primes where the reduction has a simple node. Similarly, there are practical reasons requiring us to deal with torsors that are not geometrically connected (corresponding to elements in the 'fake Selmer set' of [BS09, PS97] – see Remark 4.2), so working in this generality will pay off.

Definition 3.2. *We say that a torsor $Y \to X_{k_v}$ under G is* unramified *if the map*

$$X(k_v) \ni x_v \mapsto Y_{x_v} \in \mathrm{H}^1(k_v, G)$$

sending a point x_v to the class of the fiber above it has its image contained in the unramified subgroup. We say that an X-torsor under G is unramified at $v \in \Omega_k$ *(resp.,* unramified outside $S \subset \Omega_k$*) if its base change to $\mathrm{Spec}(k_v)$ is unramified (resp., for all $v \notin S$).*

Lemma 3.3. *Suppose $X(k_v) \neq \emptyset$ and X_{k_v} spreads out to a smooth projective scheme $\mathcal{X}_v \to \mathrm{Spec}(\mathcal{O}_v)$ and λ spreads out to a morphism $\mathcal{M}_v \to \mathrm{Pic}_{\mathcal{X}_v/\mathrm{Spec}(\mathcal{O}_v)}$ of smooth proper group schemes over $\mathrm{Spec}(\mathcal{O}_v)$. Then*

(1) There exists an unramified X_{k_v}-torsor of type λ.
(2) If $Y \to X_{k_v}$ is a torsor of type λ which spreads out to an $\mathcal{X}_v$-torsor under $\mathcal{G}_v = \mathcal{M}_v^\vee$, then $Y \to X_{k_v}$ is unramified.

Proof. Since $X_{k_v}(k_v) = \mathcal{X}_v(\mathcal{O}_v) \neq \emptyset$, the type map fits into the following commutative diagram with exact rows,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^1(k_v, G) & \longrightarrow & \mathrm{H}^1(X_v, G) & \xrightarrow{\text{type}} & \mathrm{Hom}(M, \mathrm{Pic}_{X_v}) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathrm{H}^1(\mathcal{O}_v, \mathcal{G}_v) & \longrightarrow & \mathrm{H}^1(\mathcal{X}_v, \mathcal{G}_v) & \longrightarrow & \mathrm{Hom}(\mathcal{M}, \mathrm{Pic}_{\mathcal{X}_v/\mathcal{O}_v}) & \longrightarrow & 0 \end{array}$$

where the rows come from the Leray spectral sequence as in [Sko01, Corollary 2.3.9] (see also [Ant11, Proposition 3.2] for an alternative construction of the bottom row) and the vertical arrows arise from taking generic fibers. The existence of a point is used to prove surjectivity of the type map and its counterpart over $\mathrm{Spec}(\mathcal{O}_v)$. The assumption that λ spreads out implies (using the diagram) that there is an X_{k_v}-torsor of type λ which spreads out as in (2). So, (2) $\Rightarrow$ (1).

To prove (2), note that the evaluation map $X(k_v) \to \mathrm{H}^1(k_v, G)$ factors through the evaluation map of the $\mathcal{X}_v$-torsor, so its image lies in the image of $\mathrm{H}^1(\mathcal{O}_v, \mathcal{G}_v) \to \mathrm{H}^1(k_v, G)$ which is the unramified subgroup. □

Lemma 3.4. *Suppose that $\pi : Y \to X$ is a torsor of type λ which is unramified outside S. Then*

$$X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)} = \left\{(x_v) \in X(\mathbb{A}_k) \ : \ \exists \tau \in \mathrm{H}^1_S(k, G) \text{ such that } \forall v \in S,\ x_v \in \pi^\tau(Y^\tau(k_v))\right\}.$$

Proof. For some S' containing S such that $S' - S$ is finite, G spreads out to a smooth group scheme $\mathcal{G}$ over $\mathrm{Spec}(\mathcal{O}_{k,S'})$ and $Y \to X$ spreads out to a torsor $\mathcal{Y} \to \mathcal{X}$ under $\mathcal{G}$. Then M spreads out to a smooth group scheme $\mathcal{M}$ dual to $\mathcal{G}$ and $\mathrm{H}^1_{S'}(k, M) = \mathrm{H}^1(\mathcal{O}_{k,S'}, \mathcal{M})$ and similarly for $\mathcal{G}$. Moreover, $\mathrm{H}^1_S(k, M) = \ker\left(\mathrm{H}^1(\mathcal{O}_{k,S'}, \mathcal{M}) \to \prod_{v \in S'-S} \mathrm{H}^1(k_v, M)/U_v^\perp\right)$, where $U_v^\perp$ denotes the annihilator of the unramified subgroup $U_v \subset \mathrm{H}^1(k_v, G)$ under the pairing (2.1). In this situation the generalized Poitou-Tate exact sequence [Čes15, Theorem 6.2] (see also [Cre12, Proposition 4.6] for a proof in the case of finite S' that only uses Galois cohomology) gives an exact sequence

$$\mathrm{H}^1_{S'}(k, G) \longrightarrow \prod\nolimits'_{v \in S} \mathrm{H}^1(k_v, G) \times \prod\nolimits_{v \in S'-S} \tfrac{\mathrm{H}^1(k_v, G)}{U_v} \longrightarrow \mathrm{H}^1_S(k, M)^*$$

$$(\tau_v)_{v \in S'} \longmapsto \left[\alpha \mapsto \Sigma_{v \in S'} \mathrm{inv}_v(\tau_v \cup \alpha_v)\right],$$

where the cup product is induced by the pairing in (2.1).

For $\beta \in \mathrm{Br}_{\lambda,S}(X)$ corresponding to $\alpha \in \mathrm{H}^1_S(k, M)$ and $(x_v) \in X(\mathbb{A}_k)$ we have, as in [Sko01, (6.8) on p. 121],

$$\Sigma_{v \in \Omega_k} \mathrm{inv}_v(\beta(x_v)) = \Sigma_{v \in \Omega_k} \mathrm{inv}_v(Y_{x_v} \cup \alpha_v) = \Sigma_{v \in S} \mathrm{inv}_v(Y_{x_v} \cup \alpha_v), \tag{3.1}$$

where the final equality follows from the fact that, for $v \notin S$, Y_{x_v} is unramified and $\alpha_v := \mathrm{res}_{k_v/k}(\alpha)$ is orthogonal to the unramified subgroup. Exactness of the Poitou-Tate sequence above shows that there exists $\tau \in \mathrm{H}^1_{S'}(k, G)$ with the same image as $(Y_{x_v})_{v \in S'}$ if and only if $(x_v) \in X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)}$. Note that for any such τ we have $\tau_v = Y_{x_v}$ for $v \in S$ and $\tau \in \mathrm{H}^1_S(k, G)$ because $Y_{x_v} \in U_v$ for $v \in S' - S$. By definition, $Y_{x_v} = \tau_v$ is equivalent to $x_v \in \pi^{\tau_v}(Y^{\tau_v}(k_v))$, so this proves the lemma. □

The next lemma characterizes the existence of unramified outside S torsors of type λ in terms of the Brauer-Manin obstruction.

Lemma 3.5. *Suppose that $X(\mathbb{A}_k) \neq \emptyset$ and that for every $v \notin S$ there is an unramified X_{k_v}-torsor of type λ defined over k_v. Then there exists an X-torsor of type λ unramified outside S if and only if $X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)} \neq \emptyset$.*

Remark 3.6.

(1) *By Lemma 3.3 the hypothesis is satisfied if X spreads out to a smooth proper scheme and λ spreads out to a morphism of smooth proper group schemes over $\mathrm{Spec}(\mathcal{O}_{k,S})$.*

(2) *The hypothesis is satisfied for $S = \Omega_k$, in which case the result is a crucial step in establishing the descent theory for abelian torsors (See (1) at the top of page 115 of [Sko01]). In this case the result holds more generally for $M = G^\vee$ of finite type. For*

general S we must restrict to finite M as the proof relies on the Poitou-Tate exact sequence which requires that M is finite or that S is cofinite.

Proof. First suppose there exists a torsor $Y \to X$ of type λ unramified outside S. For any $v \in \Omega_k$, any $x_v \in X(k_v)$ and any $\alpha \in Ш^1_S(k, M)$ we have $Y_{x_v} \cup \alpha_v = 0$. For $v \in S$ this is because $\alpha_v = 0$ and for $v \notin S$ this is because Y_{x_v} is unramified and hence orthogonal to α_v. If $\beta \in Б_{\lambda,S}(X)$ corresponds to α, then (3.1) shows that $X(\mathbb{A}_k)^\beta = X(\mathbb{A}_k)$. This proves one direction of the lemma.

For the converse, suppose $X(\mathbb{A}_k)^{Б_{\lambda,S}(X)} \neq \emptyset$. Then $X(\mathbb{A}_k)^{Б_\lambda(X)} \neq \emptyset$ and so there exists a torsor $Y \to X$ of type λ (cf. Remark 3.6). For some $S' \supset S$ with $S' - S$ finite, G spreads out to a smooth proper group scheme $\mathcal{G}$ over $\operatorname{Spec}(\mathcal{O}_{k,S'})$ and $Y \to X$ spreads out to a torsor $\mathcal{Y} \to \mathcal{X}$ under $\mathcal{G}$ with $\mathcal{X}$ smooth and proper over $\operatorname{Spec}(\mathcal{O}_{k,S'})$. By Lemma 3.3, $Y \to X$ is unramified outside S'.

The Cartier dual $\mathcal{M}$ of $\mathcal{G}$ has generic fiber M and

$$Ш^1_S(k, M) = \ker\left(\mathrm{H}^1(\mathcal{O}_{k,S'}, \mathcal{M}) \to \prod_{v\in S} \mathrm{H}^1(k_v, M) \times \prod_{v\in S'-S} \mathrm{H}^1(k_v, M)/U_v^\perp\right),$$

where $U_v \subset \mathrm{H}^1(k_v, G)$ is the unramified subgroup and $U_v^\perp \subset \mathrm{H}^1(k_v, M)$ is its annihilator under the pairing (2.1). The generalized Poitou-Tate sequence [Česl5, Theorem 6.2] gives

$$\mathrm{H}^1_{S'}(k, G) \to \prod_{v\in S'-S} \mathrm{H}^1(k_v, G)/U_v \to Ш^1_S(k, M)^*.$$

(We have omitted the factors at $v \in S$ in the central term as they are $\mathrm{H}^1(k_v, G)/0^\perp = \mathrm{H}^1(k_v, G)/\mathrm{H}^1(k_v, G) = 0$.) Let $(x_v) \in X(\mathbb{A}_k) = X(\mathbb{A}_k)^{Б_{\lambda,S}(X)}$. Arguing as in the proof of Lemma 3.4 using (3.1) we obtain $\tau \in \mathrm{H}^1(\mathcal{O}_{k,S'}, \mathcal{G})$ mapping to the image of $(Y_{x_v})_{v\in S'-S}$.

We claim that the twist of $Y \to X$ by τ is unramified outside S. It is unramified outside S' since both $Y \to X$ and τ are unramified outside S'. For $v \in S' - S$, we have $(Y^\tau)_{x_v} = Y_{x_v} - \tau_v \in U_v$. The image of the evaluation map $X(k_v) \to \mathrm{H}^1(k_v, G)$ given by $Y^\tau \to X$ therefore intersects the unramified subgroup. By assumption there exists an unramified torsor $Y_v \to X_{k_v}$ of type λ and the base change of $Y^\tau \to X$ to k_v is a twist of this unramified torsor. It follows that the image of the evaluation map $X(k_v) \to \mathrm{H}^1(k_v, G)$ given by $Y^\tau \to X$ lies in a coset of the unramified subgroup. As this coset has nonempty intersection with the unramified subgroup, it must be the unramified subgroup. So $Y \to X$ is unramified at $v \in S' - S$ as well. □

Lemma 3.7. *Suppose $S \subset \Omega_k$ is such that*

(1) there exists a torsor $\pi : Y \to X$ of type λ unramified outside S,
(2) for all torsors $\pi : Y \to X$ of type λ which are unramified outside S and locally soluble at all primes $v \in S$, we have $Y(\mathbb{A}_k) \neq \emptyset$.

Then the conclusion of Theorem 3.1 holds.

Proof. Since $X(\mathbb{A}_k)^{\mathrm{Br}_\lambda(X)} \subset X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)}$ it suffices to prove that

$$\rho_S\left(X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)}\right) \subset \rho_S\left(X(\mathbb{A}_k)^{\mathrm{Br}_\lambda(X)}\right),$$

where ρ_S denotes the projection map $\rho_S : X(\mathbb{A}_k) = \prod_{v\in\Omega_k} X(k_v) \to \prod_{v\in S} X(k_v)$. So let $(x_v)_{v\in S} \in \rho_S\left(X(\mathbb{A}_k)^{\mathrm{Br}_{\lambda,S}(X)}\right)$. By Lemma 3.4 there exists $\tau \in \mathrm{H}^1_S(k, G)$ such that $x_v \in$

$\pi^\tau(Y^\tau(k_v))$ for all $v \in S$. By assumption (2), $Y^\tau(\mathbb{A}_k) \neq \emptyset$. In particular, there exists $y = (y_v)_{v\in\Omega_k} \in Y^\tau(\mathbb{A}_k)$ such that $\pi^\tau(y_v) = x_v$ for $v \in S$. In other words, $(x_v)_{v\in S} = \rho_S(\pi^\tau(y))$. On the other hand

$$\pi^\tau(y) \in \bigcup_{\tau\in \mathrm{H}^1_S(k,G)} \pi^\tau(Y^\tau(\mathbb{A}_k)) \subset \bigcup_{\tau\in \mathrm{H}^1(k,G)} \pi^\tau(Y^\tau(\mathbb{A}_k)) = X(\mathbb{A}_k)^{\mathrm{Br}_\lambda(X)},$$

where the final equality is by [Sko01, Theorem 6.1.2]. So $(x_v)_{v\in S} \in \rho_S\left(X(\mathbb{A}_k)^{\mathrm{Br}_\lambda(X)}\right)$ as required. □

Proof of Theorem 3.1. Suppose the type map $\lambda : M \to \mathrm{Pic}(\overline{X})$ factors as $M \twoheadrightarrow M_0 \hookrightarrow \mathrm{Pic}(\overline{X})$. Then $G_0 := M_0^\vee \subset G$ and $\overline{Y} \to \overline{X}$ is a disjoint union of torsors $\overline{Y}_0 \to \overline{X}$ under $\overline{G}_0$ (which are torsors of type $\lambda_0 : M_0 \to \mathrm{Pic}(\overline{X})$). The Weil conjectures (or the earlier result of Lang-Weil) give an explicitly computable bound B depending only on $\overline{Y}_0 \to \overline{X}$ such that if $v \in \Omega_k$ has residue cardinality larger than B and $\mathcal{Y}_0 \to \mathrm{Spec}(\mathcal{O}_v)$ is smooth and has geometric generic fiber isomorphic to $\overline{Y}_0$, then $\mathcal{Y}_0(\mathbb{F}_v) \neq \emptyset$. By Hensel's lemma $\mathcal{Y}_0(k_v) \neq \emptyset$ as well.

There is a finite set of primes $S \subset \Omega_k$ containing all archimedean primes such that X spreads out to smooth proper scheme $\mathcal{X}$, G and M spread out to Cartier dual smooth group schemes $\mathcal{G}$ and $\mathcal{M}$ and λ spreads out to a morphism $\mathcal{M} \to \mathrm{Pic}_{\mathcal{X}/\mathcal{O}_{k,S}}$ of group schemes over $\mathrm{Spec}(\mathcal{O}_{k,S})$, where $\mathrm{Pic}_{\mathcal{X}/\mathcal{O}_{k,S}}$ is the (smooth and proper) relative Picard scheme whose existence follows from the fact that $\mathcal{X}$ is smooth and proper. Enlarge S to ensure that

(i) $Ш^1_S(k, G/G_0) = Ш^1(k, G/G_0)$,
(ii) S includes all primes of residue cardinality up to the bound B.

To see that (i) is possible, note that as $Ш^1_S(k, G/G_0) - Ш^1(k, G/G_0)$ is finite there is a finite set of primes S' containing S such that

$$Ш^1(k, G/G_0) = \ker\left(Ш^1_S(k, G/G_0) \to \prod_{v\in S'} \mathrm{H}^1(k_v, G/G_0)\right).$$

This kernel is $Ш^1_{S'}(k, G/G_0)$.

As noted in Remark 3.6, the hypothesis of Lemma 3.5 is satisfied for S. Since $Б_{\lambda,S}(X) \subset \mathrm{Br}_{\lambda,S}(X)$ we may assume that there is a torsor $Y \to X$ of type λ unramified outside S (otherwise both sets in the statement of the theorem are empty by Lemma 3.5). It will therefore suffice to verify that the second hypothesis of Lemma 3.7 is satisfied.

So, suppose $Y \to X$ is an unramified outside S torsor of type λ for which $Y(k_v) \neq \emptyset$ for $v \in S$. The scheme of connected components $\pi_0(Y)$ is a torsor under G/G_0 and the assumptions imply that $\pi_0(Y) \in Ш^1_S(k, G/G_0) = Ш^1(k, G/G_0)$. Thus $\pi_0(Y)$ is everywhere locally soluble. In particular, for any $v \notin S$, Y_v has a geometrically irreducible component defined over k_v which is an X_v-torsor under G_0. This spreads out to a smooth scheme $\mathcal{Y}_0 \to \mathrm{Spec}(\mathcal{O}_v)$ whose generic fiber is geometrically isomorphic to $\overline{Y}_0$. By (3) and the discussion in the first paragraph we conclude that $Y(k_v) \neq \emptyset$. Thus, the second hypothesis of Lemma 3.7 is satisfied. □

4. The Brauer-Manin obstruction for hyperelliptic curves

Let k be a field of characteristic 0. Given a hyperelliptic curve C/k with Jacobian J, consider the type map $\lambda_0 : J[2] = \mathrm{Pic}(\overline{C})[2] \subset \mathrm{Pic}(\overline{C})$. The main result of [CV15] is to give

explicit representatives (as corestrictions of quaternion algebras over the function field $k(C)$) for the elements in a subgroup $\mathrm{Br}_\Upsilon(C)$ of $\mathrm{Br}_{\lambda_0}(C)$ (See [CV15, Proposition 5.1]). In this section we show that, when k is a number field, this subgroup captures the obstruction to the Hasse principle coming from $\mathrm{Br}(C)[2]$. We then use the results of the previous section to give a computable description of this obstruction.

4.1. **The group $\mathrm{Br}_\Upsilon(C)$.** To begin let us give a new definition of $\mathrm{Br}_\Upsilon(C)$ as a subgroup of the form $\mathrm{Br}_\lambda(C)$ for appropriate λ. The quotient by the hyperelliptic involution defines a map $\rho : C \to \mathbb{P}^1$ which we may assume is not ramified over ∞. Let $\mathfrak{m} = \rho^*\infty \in \mathrm{Div}(C)$. The 2-torsion of the generalized Jacobian $J_\mathfrak{m} = \mathrm{Jac}(C_\mathfrak{m})$ sits in an exact sequence

$$1 \to \mu_2 \to J_\mathfrak{m}[2] \to J[2] \to 0\,. \tag{4.1}$$

Let $\lambda : J_\mathfrak{m}[2] \to \mathrm{Pic}(\overline{C})$ be the composition of λ_0 with the surjective map $J_\mathfrak{m}[2] \to J[2]$. Now define $\mathrm{Br}_\Upsilon(C) = \mathrm{Br}_\lambda(C)$. When k is a number field and $S \subset \Omega_k$ contains all archimedean primes we define $\mathrm{Br}_{\Upsilon,S}(C) = \mathrm{Br}_{\lambda,S}(C)$.

We now recall the definition in [CV15] and observe that it is equivalent (the group there is denoted $\mathrm{Br}_2^\Upsilon(C)$). The long exact sequence of Galois cohomology groups from (4.1) gives an exact sequence

$$\mathrm{H}^1(k, J_\mathfrak{m}[2]) \to \mathrm{H}^1(k, J[2]) \xrightarrow{\Upsilon} \mathrm{Br}(k)\,.$$

In [CV15] the group is defined in as $r^{-1}\left((\lambda_0)_*(\ker(\Upsilon))\right)$, where $r : \mathrm{Br}_1(C)/\mathrm{Br}_0(C) \simeq \mathrm{H}^1(k, \mathrm{Pic}(\overline{C}))$ is the canonical map. By the exact sequence above, this is equal to $\mathrm{Br}_\lambda(C) = r^{-1}(\lambda_*(\mathrm{H}^1(k, J_\mathfrak{m}[2])))$.

Theorem 4.1. *Let C be a hyperelliptic curve over a number field k. Then*

$$C(\mathbb{A}_k)^{\mathrm{Br}(C)[2]} = C(\mathbb{A}_k)^{\mathrm{Br}_{\lambda_0}(C)} = C(\mathbb{A}_k)^{\mathrm{Br}_\Upsilon(C)}\,.$$

Proof. The first equality is a special case of [CV15, Corollary 6.2]. We must prove the second. As noted above $\mathrm{Br}_\Upsilon(C) = \mathrm{Br}_\lambda(C)$, where $\lambda : J_\mathfrak{m}[2] \to J[2] \subset \mathrm{Pic}(\overline{C})$ is the composition of the quotient map in (4.1) with the inclusion $\lambda_0 : J[2] \subset \mathrm{Pic}(\overline{C})$.

A torsor $\pi : Y \to C$ of type λ is a C-torsor under the finite group scheme $(J_\mathfrak{m}[2])^\vee$, which is isomorphic to $\mathcal{J}[2] := \left(\mathrm{Pic}(\overline{C})/\langle\mathfrak{m}\rangle\right)[2]$, see [Cre20, Proposition 2.8]. The sequence (4.1) and its dual induce the vertical maps in the following commutative diagram.

$$\begin{array}{ccc}
\mathrm{H}^1(C, J[2]) & \xrightarrow{\text{type}} & \mathrm{Hom}(J[2], \mathrm{Pic}(\overline{C})) \\
\downarrow & & \downarrow \\
\mathrm{H}^1(C, \mathcal{J}[2]) & \xrightarrow{\text{type}} & \mathrm{Hom}(J_\mathfrak{m}[2], \mathrm{Pic}(\overline{C})) \qquad \lambda \\
\downarrow & & \downarrow \\
\mathrm{H}^1(C, \mathbb{Z}/2\mathbb{Z})) & \xrightarrow{\text{type}} & \mathrm{Hom}(\mu_2, \mathrm{Pic}(\overline{C})) \qquad 0
\end{array}$$

(In the top left term we have used $J[2]^\vee \simeq J[2]$.) A C-torsor under $\mathbb{Z}/2\mathbb{Z}$ whose type is the 0 map is a union of two copies of C permuted by Galois and may be identified with a class in $\mathrm{H}^1(k, \mathbb{Z}/2\mathbb{Z})$. The image of a torsor $Y \to X$ of type λ under the map $\mathrm{H}^1(C, \mathcal{J}[2]) \to \mathrm{H}^1(C, \mathbb{Z}/2\mathbb{Z})$ is the scheme of connected components of Y, which geometrically is a pair of points. A connected torsor (Y, π) of type λ must have $Y(\mathbb{A}_k) = \emptyset$, since it is geometrically

disconnected. Exactness of the first column in the diagram shows that the disconnected torsors of type λ are precisely those that are the image of a torsor of type λ_0.

A torsor $\pi_0 : Y_0 \to C$ of type λ_0 can be composed with the hyperelliptic involution $\iota : C \to C$ to obtain another torsor $\iota \circ \pi_0 : Y_0 \to C$ of type λ_0. The image of (Y_0, π_0) under the map $\mathrm{H}^1(C, J[2]) \to \mathrm{H}^1(C, \mathcal{J}[2])$ is the disjoint union of (Y_0, π_0) and $(Y_0, \iota \circ \pi_0)$. From this it follows that

$$\bigcup_{\substack{(Y_0,\pi_0)\in \mathrm{H}^1(C,J[2])\,,\\ \mathrm{type}(Y_0,\pi_0)=\lambda_0}} \pi_0(Y_0(\mathbb{A}_k)) = \bigcup_{\substack{(Y,\pi)\in \mathrm{H}^1(C,\mathcal{J}[2])\,,\\ \mathrm{type}(Y,\pi)=\lambda}} \pi(Y(\mathbb{A}_k))\,.$$

By descent theory [Sko01, Theorem 6.1.2] the term on the left is equal to $C(\mathbb{A}_k)^{\mathrm{Br}_{\lambda_0}(X)}$ and the term on the right is equal to $C(\mathbb{A}_k)^{\mathrm{Br}_{\lambda}(X)} = C(\mathbb{A}_k)^{\mathrm{Br}_{\Upsilon}(X)}$. □

Remark 4.2. *The restriction of the map* $\mathrm{H}^1(C, J[2]) \to \mathrm{H}^1(C, \mathcal{J}[2])$ *to the subset* $\mathrm{Sel}^2(C/k)$ *of locally soluble torsors is essentially the map* $\mathrm{Sel}^2(C/k) \to \mathrm{Sel}^2_{\mathrm{fake}}(C/k)$ *in* [BS09, Section 3]. *The proof of the theorem relies on the fact that this map is surjective. This follows from the fact that the underlying curves of the torsors* (Y_0, π_0) *and* $(Y_0, \iota \circ \pi_0)$ *are isomorphic.*

4.2. **The μ-map.** Suppose that C is defined by $y^2 = f(x)$ with $f(x) \in k[x]$ separable of even degree. We denote the leading coefficient of $f(x)$ by c. Define $L = k[x]/\langle f(x)\rangle$ and let $\theta \in L$ denote the image of x. Consider the μ map defined in [BS09, Section 2]

$$\mu : C(k) \to L^\times/k^\times L^{\times 2}\,,$$

which for a point $P = (a, b)$ with $b \neq 0$ is defined as $\mu(P) = (a - \theta)k^\times L^{\times 2}$. Let us further define $\mathfrak{L}_1 = \ker\left(N_{L/k} : L^\times/k^\times L^{\times 2} \to k^\times/k^{\times 2}\right)$ and let $\mathfrak{L}_c$ denote the coset of $\mathfrak{L}_1$ of elements whose norm lies in $ck^{\times 2}$ (This set is denoted H_k in [BS09]). Because $f(x) = cN_{L/k}(x - \theta)$, the image of μ is contained in $\mathfrak{L}_c$.

4.3. **Torsors of the form Y_δ.** As shown in [BS09, Section 2] corresponding to any $\delta \in \mathfrak{L}_c$ is a pair of two-coverings of C over k whose union gives a torsor $Y_\delta \to C$ of type λ. (The construction gives a pair of two-coverings because the morphism to C can be composed with the hyperelliptic involution - see the bottom of page 2351 of [BS09].)

4.4. **Cohomological interpretation.** The group scheme $\mathcal{J}[2]$ sits in a short exact sequence $1 \to \mu_2 \to \mathrm{Res}_{L/k}(\mu_2) \to \mathcal{J}[2] \to 0$ identifying it with $\mathrm{Res}_{L/k}(\mu_2)/\mu_2$, where $\mathrm{Res}_{L/k}$ denotes the restriction of scalars functor taking L-schemes to k-schemes. The corresponding long exact sequence of Galois cohomology groups together with Hilbert's theorem 90 yields the exact sequence

$$k^\times/k^{\times 2} \to \left[\mathrm{H}^1(k, \mathrm{Res}_{L/k}(\mu_2)) = L^\times/L^{\times 2}\right] \to \left[\mathrm{H}^1(k, \mathrm{Res}_{L/k}(\mu_2)/\mu_2) = \mathrm{H}^1(k, \mathcal{J}[2])\right]\,.$$

This fits together with the cohomology sequence of (4.1) to form the following commutative diagram with exact rows and columns (which is essentially [Cre20, (2.11)] or [PS97, (12)]

specialised to the present context).

(4.2)
$$\begin{array}{ccccccc}
 & & k^\times/k^{\times 2} & = & k^\times/k^{\times 2} & & \\
 & & \downarrow & & \downarrow & & \\
\mathbb{Z}/2 & \xrightarrow{d'} & \mathrm{H}^1(k, J_{\mathfrak{m}}[2]) & \longrightarrow & L^\times/L^{\times 2} & \xrightarrow{N_{L/k}} & k^\times/k^{\times 2} \\
\| & & \downarrow & & \downarrow & & \| \\
\mathbb{Z}/2 & \xrightarrow{d} & \mathrm{H}^1(k, J[2]) & \longrightarrow & \mathrm{H}^1(k, \mathcal{J}[2]) & \xrightarrow{N} & k^\times/k^{\times 2} \\
 & & \downarrow \Upsilon & & \downarrow \Upsilon' & & \\
 & & \mathrm{Br}(k) & = & \mathrm{Br}(k) & &
\end{array}$$

In particular, there is an injective map $L^\times/k^\times L^{\times 2} \hookrightarrow \mathrm{H}^1(k, \mathcal{J}[2])$.

4.5. **Pairings.** The dualities $J_{\mathfrak{m}}[2] = \mathcal{J}[2]^\vee$ and $\mathrm{Res}_{L/k}(\mu_2) = \mathrm{Res}_{L/k}(\mathbb{Z}/2)^\vee \simeq \mathrm{Res}_{L/k}(\mu_2)^\vee$ induce cup product pairings in Galois cohomology. Together with the maps in (4.2) and the identification $\mathrm{Br}(k) = \mathrm{H}^2(k, \mathbb{G}_m)$ we obtain a commutative diagram of pairings:

(4.3)
$$\begin{array}{ccccc}
\mathrm{H}^1(k, J_{\mathfrak{m}}[2]) & \times & \mathrm{H}^1(k, \mathcal{J}[2]) & \to & \mathrm{Br}(k) \\
\downarrow & & \uparrow & & \| \\
(L^\times/L^{\times 2})_{N=1} & \times & L^\times/k^\times L^{\times 2} & \to & \mathrm{Br}(k) \\
\downarrow & & \uparrow & & \| \\
L^\times/L^{\times 2} & \times & L^\times/L^{\times 2} & \to & \mathrm{Br}(k)
\end{array}$$

Here the subscript $N = 1$ is used to indicate the kernel of the norm map. The bottom pairing is given explicitly by $\langle \ell, \ell' \rangle = \mathrm{Cor}_{L/k}(\ell, \ell')_L$, where $(\ell, \ell')_L$ denotes the quaternion algebra over L determined by ℓ and ℓ'. That this induces a well defined pairing in the middle row follows from the fact that $\mathrm{Cor}_{L/k}(\ell, a)_L = (N_{L/k}(\ell), a)_k \in \mathrm{Br}(k)$, for any $a \in k^\times$ and $\ell \in L^\times$ (see [GS06, Proposition 3.4.10(3)]).

Lemma 4.3. *Let $\delta \in \mathfrak{L}_c$ and $Y_\delta \to C$ be the corresponding torsor of type λ. The image of the evaluation map $C(k) \to \mathrm{H}^1(k, \mathcal{J}[2])$ given by $Y_\delta \to C$ is $\delta^{-1}\mu(C(K)) \subset L^\times/K^\times L^{\times 2} \subset \mathrm{H}^1(k, \mathcal{J}[2])$.*

Proof. Evaluating the torsor $Y_\delta \to C$ at $P \in C(k)$ gives the class $\tau \in \mathrm{H}^1(k, \mathcal{J}[2])$ of the fiber of Y_δ above P. Alternatively, τ is uniquely determined by the property that the point P lifts to the twist of Y_δ by τ. We will show that $\tau = \mu(P)/\delta$. By construction, a point $P \in C(k)$ lifts to Y_δ if and only if $\mu(P) = \delta$. Moreover, if $\delta' \in \mathfrak{L}_1 \subset \mathrm{H}^1(k, \mathcal{J}[2])$, then the twist of Y_δ by δ' is $Y_{\delta\delta'} \to C$. It follows that P lifts to the twist of $Y_\delta \to C$ by $\mu(P)/\delta$ as required. □

4.6. **Computable description of $C(\mathbb{A}_k)^{\mathrm{Br}(C)[2]}$.**

Theorem 4.4. *Let $C : y^2 = f(x)$ be a locally soluble hyperelliptic curve over a number field k of genus g with $f(x) \in \mathcal{O}_k[x]$. Suppose that $S \subset \Omega_k$ contains*

- *all archimedean primes,*
- *all primes above 2,*
- *all primes that divide the leading coefficient of $f(x)$,*
- *all primes v such that $\mathrm{val}_v(\mathrm{disc}(f(x))) \geq 2$,*

and that $Ш^1_S(k,\mu_2)=0$. *Then*

(1) *An adelic point* $(P_v)\in C(\mathbb{A}_k)$ *lies in* $C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(X)}$ *if and only if there exists a two-covering* $\pi: Y\to C$ *unramified outside* S *such that for all* $v\in S$, $\pi(Y(k_v))$ *contains either* P_v *or* $\iota(P_v)$. *In particular,* $C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(X)}\neq\emptyset$ *if and only if there exists a two-covering of* C *that is unramified outside* S *and soluble at all primes of* S.

(2) *If* S *contains all primes whose residue cardinality* q *satisfies*

$$\sqrt{q}+\frac{1}{\sqrt{q}}\leq 2(2^{2g}(g-1)+1)\,,$$

then

$$C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(C)}=\emptyset \quad\Leftrightarrow\quad C(\mathbb{A}_k)^{\mathrm{Br}(C)[2]}=\emptyset \quad\Leftrightarrow\quad \mathrm{Sel}^2(C/k)=\emptyset\,.$$

Proof. To prove (1), first suppose there is a two-covering $\pi: Y\to C$ with the stated property. Composing with the hyperelliptic involution gives another such torsor and the union of these is a torsor of type $\lambda: J_{\mathfrak{m}}[2]\to \mathrm{Pic}(\overline{X})$ that is unramified outside S and which contains a lift of P_v for every $v\in S$. By Lemma 3.4 we conclude that $(P_v)\in C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(C)}$.

For the converse, suppose $(P_v)\in C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(C)}\neq\emptyset$. For $v\notin S$ it follows from [BS09, Lemma 4.3] that there exists an unramified C_{k_v}-torsor of type λ. Indeed, the lemma shows that the image of $\mu: C(k_v)\to L_v^\times/k_v^\times L_v^{\times 2}\subset \mathrm{H}^1(k_v,\mathcal{J}[2])$ lies in the unramified subgroup. Given δ_v in the image, the corresponding torsor $Y_{\delta_v}\to C_v$ is unramified by Lemma 4.3. By Lemma 3.5 we thus conclude that there exists a C-torsor of type λ that is unramified outside S (note that $(P_v)\in C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(C)}\subset C(\mathbb{A}_k)^{\mathrm{B}_{\lambda},S(C)}$). This shows that the hypothesis of Lemma 3.4 is satisfied and so we may conclude that there is a torsor of type λ unramifed outside S which contains a lift of P_v for each $v\in S$. The scheme of connected components of this torsor represents an element of $Ш^1_S(k,\mu_2)$. By assumption $Ш^1_S(k,\mu_2)=0$, so its geometric components are defined over k. These components are two-coverings of C which differ by the hyperelliptic involution. If P_v lifts to one of them, then $\iota(P_v)$ lifts to the other.

Now let us prove (2). It is well known that $\mathrm{Sel}^2(C)=\emptyset\Leftrightarrow C(\mathbb{A}_k)^{\mathrm{Br}\lambda_0(C)}=\emptyset$ (see [Sko01, Theorem 6.1.2]) and $C(\mathbb{A}_k)^{\mathrm{Br}\lambda_0(C)}=C(\mathbb{A}_k)^{\mathrm{Br}(C)[2]}=C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon(C)}$ by Theorem 4.1. If $C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(C)}=\emptyset$, then all three sets in the statement are empty. So suppose $C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon,S(C)}\neq\emptyset$. By the preceding discussion it will suffice to show that $C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon(C)}\neq\emptyset$. For this we use Lemma 3.7. Above we have shown that there is a torsor $Y\to C$ of type $\lambda: J_{\mathfrak{m}}[2]\to\mathrm{Pic}(\overline{X})$ unramified outside S, verifying the first assumption in Lemma 3.7. To verify the second suppose that $Y\to C$ is a torsor of type λ unramified outside S and soluble on S. Let $v\notin S$. We must show that $Y(k_v)\neq\emptyset$.

For any $\delta\in\mu(C(k_v))$, the proof of [BS09, Lemma 4.3] shows that the corresponding torsor $Y_\delta\to C_v$ has $Y_\delta(k_v)\neq\emptyset$ (This is where the bound on the residue cardinality of v in the hypothesis is used). It will therefore suffice to show that our Y above is isomorphic over k_v to one of the form Y_δ. Note that $Y\to C$ is a twist of $Y_\delta\to C$ by an element $\tau\in\mathrm{H}^1(k_v,\mathcal{J}[2])$ in the image of $\mathrm{H}^1(k_v,J[2])$, since both are disconnected C-torsors under $\mathcal{J}[2]=J_{\mathfrak{m}}[2]^\vee$ defined over k_v. The computation in [BS09, Lemma 4.3] shows that the image I of the evaluation map $Y_\delta: C(k_v)\to\mathrm{H}^1(k_v,\mathcal{J}[2])$ is equal to the set of elements in $\ker(\Upsilon')\cap\ker(N)=\mathfrak{L}_{v,1}$ that are unramified, where N and Υ' are the maps in (4.2) (again, using that the residue cardinality is sufficiently large). The image of the evaluation map corresponding to the twist Y is the coset τI. Since $Y\to C$ is unramified at v, τI is contained in the unramified subgroup of $\mathrm{H}^1(k_v,\mathcal{J}[2])$, and so τ itself is unramified. By

[Cre20, Lemma 2.10] $\Upsilon'(\tau) = \tau \cup d'(1)$. Since $f(x)$ has discriminant of valuation ≤ 1, $f(x)$ has a root over k_v^{unr} (see the proof of [BS09, Lemma 4.3]). This implies that $d'(1)$ is unramified and, hence, that $\Upsilon'(\tau) = \tau \cup d'(1) = 0$ because the unramified subgroups are orthogonal. From the diagram (4.2) we conclude that τ is the image of some $\delta' \in L_v^\times / L_v^{\times 2}$ which is unramified and of square norm. Then $\delta\delta'$ is unramified with norm in $ck_v^{\times 2}$ and so $Y = (Y_\delta)^\tau = Y_{\delta\delta'}$ is of the required form. □

Remark 4.5. *Suppose S is any set of primes as in the first part of Theorem 4.4. Let $v \notin S$, let $\delta \in L_v^\times$ be an unramified element of norm c times a square and let Y_δ be the corresponding torsor of type λ. In the course of the proof we have shown the following: if the evaluation map corresponding to Y_δ surjects onto the set of unramified elements in the subgroup $\ker(\Upsilon') \cap \ker(N) \subset \mathrm{H}^1(k_v, \mathcal{J}[2])$, then any torsor $Y \to C$ of type λ which is unramified outside S and soluble on S is also soluble at v. For such v it follows from Lemma 3.4 that*

$$C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon, S(C)} \neq \emptyset \quad \Leftrightarrow \quad C(\mathbb{A}_k)^{\mathrm{Br}\Upsilon, S\cup\{v\}(C)} \neq \emptyset\,.$$

The condition is satisfied at v when the reside cardinality is larger than the bound in the statement of Theorem 4.4, but it is typically also satisfied for many primes outside S below the bound as well. This observation is quite useful in practice as it allows us to identify (and safely omit) such primes from the computation.

Remark 4.6. *For any number field k, $Ш^1(k, \mu_2) = 0$ by the Grunwald-Wang theorem. It follows (cf. the proof of Theorem 3.1) that one can always enlarge S if necessary to ensure that $Ш^1_S(k, \mu_2) = 0$ as in the hypothesis of Theorem 4.4. In the case $k = \mathbb{Q}$, we have $Ш^1_S(\mathbb{Q}, \mu_2) = 0$ for any S containing the archimedean prime, but this is not true in general. For example, if $k = \mathbb{Q}(\sqrt{34})$, v is the prime above 2 and $S = \{v, \infty_1, \infty_2\}$, then $k_v = \mathbb{Q}_2(\sqrt{2})$ so the class of 2 is a nontrivial element in $Ш^1_S(k, \mu_2) \subset \mathrm{H}^1(k, \mu_2) = k^\times / k^{\times 2}$. Note however, that 3 splits in $\mathcal{O}_k$ and $2 \notin \mathbb{Q}_3^{\times 2}$. If S is enlarged to include a prime above 3, then $Ш^1_S(k, \mu_2) = 0$.*

For the remainder of the section we suppose C/k is the hyperelliptic curve defined by the affine equation $y^2 = f(x)$ and maintain the notation introduced above.

4.7. **Explicit representatives for $\mathrm{Br}_\Upsilon(C)$.** By [CV15, Proposition 5.1] the homomorphism

$$L^\times \ni \ell \mapsto \mathcal{A}_\ell := \mathrm{Cor}_{L/k}(\ell, x - \theta) \in \mathrm{Br}(k(C)) \tag{4.4}$$

induces a surjective map

$$\mathfrak{L}_1 \to \mathrm{Br}_\Upsilon(C)/\mathrm{Br}_0(C)\,.$$

4.8. **The unramified outside S subgroup.**

Definition 4.7. *Suppose that k is number field. A class in $L^\times/L^{\times 2}$ is* unramified at *$v \in \Omega_k$ if its image under the isomorphism $L^\times/L^{\times 2} = \mathrm{H}^1(k, \mathrm{Res}_{L/k}(\mu_2))$ is unramified at v. A class in $L^\times/k^\times L^{\times 2}$ is* unramified at *$v \in \Omega_k$ if its image under the injecitve map $L^\times/k^\times L^{\times 2} \to \mathrm{H}^1(k, \mathrm{Res}_{L/k}(\mu_2)/\mu_2) = \mathrm{H}^1(k, \mathcal{J}[2])$ is unramified at v. For a subset $S \subset \Omega_k$ we use $(L^\times/L^{\times 2})_S$, $\mathfrak{L}_{1,S}$ and $\mathfrak{L}_{c,S}$ to denote the subsets (of $L^\times/L^{\times 2}$, $\mathfrak{L}_1$ and $\mathfrak{L}_c$) of elements that are unramified at all primes outside of S.*

Lemma 4.8. *Suppose k is a number field. For any $S \subset \Omega_k$ satisfying the hypothesis of Theorem 4.4, the map in (4.4) induces a surjective map*

$$\mathfrak{L}_{1,S} \to \mathrm{Br}_{\Upsilon,S}(C)/\mathrm{Br}_0(C)\,.$$

Proof. Let $v \notin S$. To begin, let us observe that an element of $\mathrm{H}^1(k_v, J_{\mathfrak{m}}[2])$ is unramified if and only if its image in $L_v^\times/L_v^{\times 2}$ is unramified. To see this we use exactness of the top row of (4.2) and the fact, noted in the proof of Theorem 4.4, that $d'(1) \in \mathrm{H}^1(k_v, J_{\mathfrak{m}}[2])$ is unramified.

Now suppose $\ell' \in L^\times$ represents a class in $\mathfrak{L}_{1,S}$. Then there exists $a \in k^\times$ such that the class of $\ell = a\ell'$ lies in $(L^\times/L^{\times 2})_S$. Note that $\mathcal{A}_\ell = \mathcal{A}_{\ell'} + \mathcal{A}_a = \mathcal{A}_{\ell'} + \mathrm{Cor}_{L/k}(a, x-\theta) = \mathcal{A}_{\ell'} + (a, N_{L/k}(x-\theta)) = \mathcal{A}_{\ell'} + (a,c) \in \mathcal{A}_{\ell'} + \mathrm{Br}_0(C)$ (here $c \in k^\times$ is the leading coefficient of $f(x) = cN_{L/k}(x-\theta)$). Exactness of (4.2) shows that there exists $\alpha \in \mathrm{H}^1(k, J_{\mathfrak{m}}[2])$ mapping to the class of ℓ. By the observation in the first paragraph of the proof, $\alpha \in \mathrm{H}^1_S(k, J_{\mathfrak{m}}[2])$. The proof of [CV15, Proposition 5.1] shows that $r(\mathcal{A}_\ell) = \lambda_*(\alpha)$, so $\mathcal{A}_\ell \in \mathrm{Br}_{\Upsilon,S}(C)$.

To show surjectivity, suppose $\beta \in \mathrm{Br}_{\Upsilon,S}(C)$. Then there exists $\alpha \in \mathrm{H}^1_S(k, J_{\mathfrak{m}}[2])$ such that $r(\beta) = \lambda_*(\alpha)$ in $\mathrm{H}^1(k, \mathrm{Pic}(\overline{C}))$. If ℓ represents the image of α in $L^\times/L^{\times 2}$, then $r(\mathcal{A}_\ell) = \lambda_*(\alpha)$ so β and $\mathcal{A}_\ell$ determine the same class modulo $\mathrm{Br}_0(C)$. To prove surjectivity we must show that the image of ℓ in $L^\times/L^{\times 2}$ is unramified at v.

By assumption α annihilates the unramified subgroup of $\mathrm{H}^1(k_v, \mathcal{J}[2])$. From (4.3) it follows that the class of ℓ in $L_v^\times/L_v^{\times 2}$ annihilates the unramified subgroup of $L_v^\times/L_v^{\times 2}$. For an odd prime such as $v \notin S$, the unramified subgroup of $L_v^\times/L_v^{\times 2}$ is its own exact annihator (even when some simple factors L_i of L are ramified over k). So the class of ℓ is unramified as required. □

4.9. **Evaluation of $\mathcal{A}_\ell$.** Given $\mathcal{A} \in \mathrm{Br}(C)$ and a point $P : \mathrm{Spec}(k) \to C \in C(k)$, the evaluation of $\mathcal{A}$ at P, denoted by $\mathcal{A}(P)$, is defined as the pullback $P^*\mathcal{A} \in \mathrm{Br}(k)$.

Lemma 4.9. *Let $\ell \in (L^\times/L^{\times 2})_{N=1}$ and $P \in C(k)$. Then $\mathcal{A}_\ell(P) = \mathrm{Cor}_{L/k}(\ell, \mu(P)) \in \mathrm{Br}(k)$.*

Proof. This follows from the definition of $\mathcal{A}_\ell$ and the definition of μ given in Section 4.2. □

Lemma 4.10. *Suppose k is a local field of characteristic 0, $\ell \in (L^\times/L^{\times 2})_{N=1}$ and $P \in C(k)$. Write $L = \prod_{i=1}^n L_i$ as a product of finite extensions of k and let $\ell = (\ell_i)$ and $\mu(P) = (m_i)$ be the images under this decomposition. Then*

$$\mathrm{inv}_k(\mathcal{A}_\ell(P)) = \sum_{i=1}^n (\ell_i, m_i)_{L_i},$$

where $(\ell, m_i)_{L_i} \in \{0, 1/2\} \subset \mathbb{Q}/\mathbb{Z}$ is the (additive) Hilbert symbol on the local field L_i.

Proof. By Lemma 4.9,

$$\mathrm{inv}_k(\mathcal{A}_\ell(P)) = \mathrm{inv}_k(\mathrm{Cor}_{L/k}(\ell, \mu(P))) = \sum_{i=1}^n \mathrm{inv}_k(\mathrm{Cor}_{L_i/k}(\ell_i, m_i))\,,$$

and $\mathrm{inv}_k(\mathrm{Cor}_{L_i/k}(\ell_i, m_i)) = \mathrm{inv}_{L_i}(\ell, m_i) = (\ell, m_i)_{L_i}$, since $\mathrm{inv}_k \circ \mathrm{Cor}_{L_i/k} = \mathrm{inv}_{L_i}$ for the extension of local fields L_i/k. □

Lemma 4.11. *Suppose k is a number field and $S \subset \Omega_k$ is a finite set of primes satisfying the hypothesis of Theorem 4.4. Suppose $\ell \in (L^\times/L^{\times 2})_S$ has square norm and $(P_v) \in C(\mathbb{A}_k)$. Then*

$$\sum_{v\in\Omega_k} \mathrm{inv}_v(\mathcal{A}_\ell(P_v)) = \sum_{v\in S}(\ell, \mu_v(P_v))_v\,.$$

where $\mu_v : C(k_v) \to L_v^\times/k_v^\times L_v^{\times 2}$ is the map from Section 4.2 and $(\ell, \mu_v(P_v))_v$ is the sum of the Hilbert symbols on the simple factors of L_v.

Proof. Any $\ell \in (L^\times/L^{\times 2})_S$ is unramified at all $v \notin S$, and by [BS09, Lemma 4.3], $\mu_v(P_v)$ is unramified at all $v \notin S$ (as per the discussion in proof of 4.4). Thus, $\mathrm{inv}_v(\mathcal{A}_\ell(P_v)) = 0$ at all $v \notin S$. So

$$\sum_{v\in\Omega_k} \mathrm{inv}_v(\mathcal{A}_\ell(P_v)) = \sum_{v\in S} \mathrm{inv}_v(\mathcal{A}_\ell(P_v))\,.$$

The result follows from Lemma 4.10.

□

5. The algorithm

Let $C : y^2 = f(x)$ be a locally soluble hyperelliptic curve over a number field k of genus g with $f(x) \in \mathcal{O}_k[x]$. Let $S_{\min} \subset \Omega_k$ be a finite set of primes containing

- all archimedean primes,
- all primes above 2,
- all primes that divide the leading coefficient of $f(x)$,
- all primes v such that $\mathrm{val}_v(\mathrm{disc}(f(x))) \geq 2$, and
- enough primes so that $Ш^1_S(k, \mu_2) = 0$.

Algorithm 5.1. *Let C/k be as at the beginning of this section. Let $\ell_1, \ldots, \ell_n \in L^\times$ be elements of square norm.*

(1) Let $S \subset \Omega_k$ be the set of primes obtained by adding to $S_{\min}$ all primes where some ℓ_i is ramified.

(2) For $i = 1, \ldots, n$ compute the $\mathbb{F}_2$-linear map

$$\phi_i : \prod_{v\in S} L_v^\times/k_v^\times L_v^{\times 2} \ni (m_v) \mapsto \sum_{v\in S} \mathrm{inv}_v\langle \ell_i, m_v\rangle_v \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}\,,$$

where $\langle \ell_i, m_v\rangle_v = \mathrm{Cor}_{L_v/k_v}(\ell_i, m_v) \in \mathrm{Br}(k_v)$ denotes the central pairing in (4.3) (over the base field k_v).

(3) For $v \in S$ compute the image I_v of the map

$$\mu_v : C(k_v) \to L_v^\times/k_v^\times L_v^{\times 2}\,,$$

defined in Section (4.2).

(4) Compute and return the intersection of $\prod_{v\in S} I_v$ and $\cap_{i=1}^n \ker(\phi_i)$.

Proposition 5.2. *The output of Algorithm 5.1 is the set $\prod_{v\in S} \mu_v(\pi_v(C(\mathbb{A}_k)^B))$, where $B \subset \mathrm{Br}(C)$ is the subgroup generated by the algebras $\mathcal{A}_{\ell_1}, \ldots, \mathcal{A}_{\ell_n}$ corresponding to $\ell_1, \ldots, \ell_n$ and $\pi_v : C(\mathbb{A}_k) = \prod_{v\in\Omega_k} C(k_v) \to C(k_v)$ is the canonical projection. In particular,*

(1) the output is the empty set if and only if $C(\mathbb{A}_k)^B = \emptyset$, and

(2) *if $\ell_1, \dots, \ell_n$ represent a basis for $\mathfrak{L}_{1,S}$, then the output is the empty set if and only if $C(\mathbb{A}_k)^{\mathrm{Br}_{\Upsilon,S}(C)} = \emptyset$.*

Proof. An element $(m_v)_{v\in S} \in \prod_{v\in S} L_v^\times/k_v^\times L_v^{\times 2}$ lies in $\prod_{v\in S} I_v$ if and only if there exists $(P_v) \in C(\mathbb{A}_k)$ such that $m_v = \mu_v(P_v)$ for $v \in S$. For such (P_v), Lemmas 4.10 and 4.11 give

$$\sum_{v\in\Omega_k} \mathrm{inv}_v\, \mathcal{A}_{\ell_i}(P_v) = \sum_{v\in S} \mathrm{inv}_v\, \mathrm{Cor}_{L_v/k_v}(\ell_i, \mu_v(P_v)) = \sum_{v\in S} \mathrm{inv}_v\langle \ell_i, \mu_v(P_v)\rangle = \phi_i((m_v))\,.$$

So $P \in \cap_{i=1}^n C(\mathbb{A}_k)^{\mathcal{A}_{\ell_i}} = C(\mathbb{A}_k)^B$ if and only if $(m_v) \in \cap_{i=1}^n \ker(\phi_i)$, in which case $(m_v) \in \prod_{v\in S} \mu_v(\pi_v(C(\mathbb{A}_k)^B))$.

Statement (1) follows immediately. For (2), suppose $\{\ell_1, \dots, \ell_n\}$ represent a basis for $\mathfrak{L}_{1,S}$. Then $B \subset \mathrm{Br}_{\Upsilon,S}(C)$ and by Lemma 4.8 we have that B surjects onto $\mathrm{Br}_{\Upsilon,S}(C)/\mathrm{Br}_0(C)$. So $C(\mathbb{A}_k)^B = C(\mathbb{A}_k)^{\mathrm{Br}_{\Upsilon,S}(C)}$ and (2) follows. □

We now provide details of how to carry out the steps in the algorithm above.

Step (1): For an odd prime v one can detect whether ℓ_i is ramified at v by looking at the valuations of (the components of) ℓ_i at the primes above v, so this step is straightforward provided we can factor the numerator and denominator of the norm $N_{L/\mathbb{Q}}(\ell_i)$. In practice, we often choose S and then find $\ell_1, \dots, \ell_n$ that are unramified outside S to use as the input.

Step (2): As noted in Lemma 4.10, the pairings $\mathrm{inv}_v\langle \ell_i, m_v\rangle_v$ can be computed using Hilbert symbols. We choose a basis for each of the finite $\mathbb{F}_2$ vector spaces $L_v^\times/k_v^\times L_v^{\times 2}$ and compute the pairings of these basis elements with ℓ_i. This allows us to write down a matrix (column vector) representing the linear map ϕ_i.

Step (3): An efficient algorithm for this is described in [BS09, Section 4].

Step (4): The set to be computed is the intersection of the subspace $\cap\ker(\phi_i)$ of the finite vector space $V := \prod_{v\in S} L_v^\times/k_v^\times L_v^{\times 2}$ over $\mathbb{F}_2$ with a finite subset $I := \prod_{v\in S} I_v \subset V$. While this is clearly computable, $\#I$ grows exponentially with $\#S$, so the naive approach of testing each element of I for membership of W will quickly become impractical. We describe a recursive method for computing this intersection which makes use of the fact that the ϕ_i are sums linear maps on the $L_v^\times/k_v^\times L_v^{\times 2}$ and I is a product of subsets of these spaces.

Call a subset $X \subset \prod_{v\in S} L_v^\times/k_v^\times L_v^{\times 2}$ a subproduct if it is a Cartesian product of subsets $X = \prod_{v\in S} X_v$ with $X_v \subset L_v^\times/k_v^\times L_v^{\times 2}$. For example, I is a subproduct. Suppose $\ell \in L^\times$ is unramified outside S. For each $v \in S$, ℓ determines a partition $X_v = X_v^0 \cup X_v^1$ where $X_v^0 = \{m_v \in X_v \ : \ \mathrm{inv}_v\langle \ell, m_v\rangle = 0\}$. It follows that $X^\ell := X \cap \ker(\phi_\ell)$ is the union the $2^{(\#S-1)}$ (possibly empty) subproducts $X_{\mathbf{a}} := \prod_{v\in S} X_v^{a_v}$, where $\mathbf{a} = (a_v) \in (\mathbb{F}_2)^S$ is such that $\sum a_v = 0$. Now if $\ell' \in L^\times$ is another element unramified outside S, we see

$$X^{\{\ell,\ell'\}} = X^\ell \cap X^{\ell'} = \bigcup_{\mathbf{a}} (X_{\mathbf{a}} \cap X^{\ell'}) = \bigcup_{\mathbf{a}} (X_{\mathbf{a}})^{\ell'}\,, \tag{5.1}$$

where the sets $(X_{\mathbf{a}})^{\ell'}$ are themselves unions of $2^{(\#S-1)}$ subproducts by the argument above, which applies because the $X_{\mathbf{a}}$ are subproducts. It follows that $I^{\{\ell_1,\dots,\ell_n\}} = I \cap (\cap_{i=1}^n \ker(\phi_i))$ can be written as a union of $2^{(\#S-1)^n}$ subproducts. These may be viewed as the leaves of a regular $(\#S-1)$-ary tree of height n whose nodes at height m correspond to the subproducts in $I^{\{\ell_1,\dots,\ell_m\}}$ (the root of the tree is I and lies at height 0). To determine which of the leaves correspond to nonempty subproducts we traverse each branch upward until we reach either an empty node (i.e. node whose subproduct is empty) in which case all nodes above this are

empty, or find a nonempty node at level n in which case the corresponding elements lie in $I^{\{\ell_1,\dots,\ell_n\}}$.

Let us discuss the efficiency of this approach. Since the dimension of $L_v^\times/k_v^\times L_v^{\times 2}$ is bounded by a constant c independent of v, computing the nodes $X_{\mathbf{a}}$ comprising X^ℓ below a given node X requires checking subspace membership for at most $\sum_{v\in S}\#X_v \le c\#S$ elements (this is linear in $\#S$, whereas the naive approach would require $\prod_{v\in S}\#X_v$ membership checks, which is exponential in $\#S$). In a worst case scenario where all interior nodes are nonempty (so we must traverse the entire tree) we would need to call the procedure $2^{(\#S-1)^n}$ times. In practice though, the situation is much better. For given ℓ, there are typically very few nodes $X_{\mathbf{a}}\subset X^\ell$ which are nonempty, meaning most branches are quite short. In part this is explained by the following observation: the sets X_v^1 are empty except possibly when v lies in the set

$$S'(\ell) := \{v\in S \ : \ \ell \text{ is ramified at } v,\ v\mid 2c,\ v \text{ is archimedean, or } \operatorname{ord}_v(\operatorname{disc}(f))\ge 2\}\ ,$$

which is typically much smaller than S. This is because for primes $v\notin S'(\ell)$ both the image of ℓ in $L_v^\times/L_v^{\times 2}$ and the local image I_v are unramified (cf. the proof of Theorem 4.4).

5.1. **Choosing the input for Algorithm 5.1.** Suppose $S\subset\Omega_k$ contains $S_{\min}$ and let $B\subset \operatorname{Br}(C)$ be the subgroup generated by $\mathcal{A}_{\ell_1},\dots,\mathcal{A}_{\ell_n}$, where $\ell_1,\ell_2,\dots,\ell_n\in L^\times$ are elements of square norm unramified outside S. The algorithm allows us to determine if $C(\mathbb{A}_k)^B$ is empty. We have containments

$$C(k)\subset C(\mathbb{A}_k)^{\operatorname{Br}(C)[2]}\subset C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S}(C)}\subset C(\mathbb{A}_k)^B\subset C(\mathbb{A}_k)\,.$$

If $\{\ell_1,\dots,\ell_n\}$ spans $\mathfrak{L}_{1,S}$, then Lemma 4.8 shows that $C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S}(C)}=C(\mathbb{A}_k)^B$. As described in [PS97, Section 12], a basis for $\mathfrak{L}_{1,S}$ can be computed from the S-class and S-unit groups of the rings of integers of the simple factors of L. In practice this may only be feasible under the assumption of GRH. The standard algorithms used to compute class and unit groups will produce a basis for a subspace of $\mathfrak{L}_{1,S}$, which is equal to $\mathfrak{L}_{1,S}$ under the assumption of GRH. Consequently, if $\ell_1,\dots,\ell_n$ is such a conditional basis, the equality $C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S}(C)}=C(\mathbb{A}_k)^B$ is conditional on GRH, but the containment $C(k)\subset C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S}(C)}\subset C(\mathbb{A}_k)^B$ is not. In particular, if we conclude from Algorithm 5.1 that $C(\mathbb{A}_k)^B=\emptyset$, then it follows unconditionally that $C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S}(C)}=C(k)=\emptyset$.

By Theorem 4.4, the containment $C(\mathbb{A}_k)^{\operatorname{Br}(C)[2]}\subset C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S}(C)}$ becomes an equality provided S contains all primes of norm up to the bound in the theorem (which depends on the genus of C). Consequently, Algorithm 5.1 gives an algorithm to check if $C(\mathbb{A})^{\operatorname{Br} C[2]}=\emptyset$. Including all primes up to that bound quickly becomes impractical (the bounds are 1158, 66562, 2365446, for $g=2,3,4$). However, in practice we have found that examples with

$$C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S_{\min}}(C)}\neq\emptyset \quad \text{ and } C(\mathbb{A}_k)^{\operatorname{Br}_{\Upsilon,S}(C)}=\emptyset$$

are fairly uncommon. In such cases, one usually finds that this holds with S including only primes of bad reduction and primes well below the bound in Theorem 4.4. Among the samples described in the following section we found only one curve where including a prime of good reduction larger than 100 had an impact; this genus 5 curve is considered in Section 6.1 below. This behavior is similar to that seen in the descent algorithm of [BS09], as can be explained by Theorem 4.4(1) (see also Remark 4.5). The descent algorithm computes the finite set of two-coverings locally soluble outside $S_{\min}$ (conditionally on GRH) and then

checks these for local solubility at the primes below the bound. Only the primes where one of these coverings is not soluble will be relevant for the Brauer-Manin obstruction.

For curves of high genus or with large coefficients computation of $\mathfrak{L}_{1,S}$ may be prohibitive even assuming GRH. In this case we may still be able to compute some elements of $\mathfrak{L}_{1,S}$ which may be enough to show $C(\mathbb{A}_k)^B = \emptyset$, allowing us to conclude that $C(k) = \emptyset$ (for an example see Proposition 6.2). In fact, the standard algorithm for computing $\mathfrak{L}_{1,S}$ proceeds by generating random elements until sufficiently many have been found (assuming GRH gives a better stopping criterion). Computing the obstructions coming from such randomly generated elements may lead to a more efficient Las Vegas style algorithm for computing Brauer-Manin obstructions. This idea will be pursued elsewhere.

6. Examples and Data

6.1. **A genus 5 example.** Consider the genus 5 curve $C/\mathbb{Q}$ defined by $y^2 = f(x)$, where

$$f(x) = -17x^{12} - 13x^{11} - 15x^{10} + 6x^9 - 19x^8 + 5x^7 - 19x^6 + 4x^5 - 2x^4 + 19x^3 + 12x^2 + 13x - 6\,.$$

This curve is everywhere locally soluble. The discriminant of $f(x)$ factors as

$$\operatorname{disc}(f(x)) = 2^6 \times 5^2 \times 29 \times 151 \times 54918937 \times 571571633 \times 8389309314807991\,,$$

so we have $S_{\min} = \{2, 5, 17, \infty\}$. Under the assumption of GRH we can compute a basis for $\mathfrak{L}_{1,S_{\min}}$ in a couple of seconds. Let $B \subset \operatorname{Br}_{\Upsilon,S_{\min}}(C)$ denote the subgroup spanned by this conditional basis. Using Algortihm 5.1 we compute the image of the set $C(\mathbb{A}_{\mathbb{Q}})^B$ in $\prod_{v\in S_{\min}} L_v^\times/k_v^\times L_v^{\times 2}$ and find that it is not empty. This does not imply $C(\mathbb{A}_{\mathbb{Q}})^{\operatorname{Br}(C)[2]} \neq \emptyset$ (even assuming GRH) because we have not considered elements in $\operatorname{Br}_\Upsilon(C)$ that ramify only at the primes below the bound in Theorem 4.4(2), which in this case is 67141638. To obtain a deeper obstruction we can repeat the computation, replacing $S_{\min}$ by $S_N := S_{\min} \cup \{p \leq N \ : \ p \text{ is prime}\}$ for a suitable bound N. In practice $N = 1000$ is entirely feasible and we found that $C(\mathbb{A}_{\mathbb{Q}})^{\operatorname{Br}_{\Upsilon,S_{1000}}(C)} = \emptyset$, proving that C is a counterexample to the Hasse principle. The entire computation took about 12 minutes on our server.

As we have found is typically the case, the obstruction can also be obtained using a much smaller set of primes S. The `TwoCoverDescent` in Magma described in [BS09] computes the sets

$$\operatorname{Sel}^2(C/\mathbb{Q})_N := \{\text{Two-covers that are locally soluble for all } p \leq N \text{ and all } p > 67141638\}$$

for increasing N. After about 20 minutes on our server it concluded that $\operatorname{Sel}^2(C/\mathbb{Q})_{238} \neq \emptyset$, but $\operatorname{Sel}^2(C/\mathbb{Q})_{239} = \emptyset$ (conditionally on GRH). In light of Theorem 4.4, we therefore expect the prime $p = 239$ will be relevant for the Brauer-Manin obstruction as well. Running Algorithm 5.1 with a (GRH-conditional) basis for $\mathfrak{L}_{1,S}$, with $S = \{2, 5, 17, 239, \infty\}$ takes about 15 seconds and shows unconditionally that the sets $C(\mathbb{Q})$, $C(\mathbb{A}_{\mathbb{Q}})^{\operatorname{Br}(C)[2]}$, $C(\mathbb{A}_{\mathbb{Q}})^{\operatorname{Br}_{\Upsilon,S}(C)}$ and $\operatorname{Sel}^2(C/\mathbb{Q})_{239}$ are all empty. In this way, Algorithm 5.1 can be used to certify the otherwise conditional output of `TwoCoverDescent`. That said, in the vast majority of cases where we have seen a Brauer-Manin obstruction it is already given by $\operatorname{Br}_{\Upsilon,S_{\min}}(C)$ and (for higher genus curves at least) it seems computation of $C(\mathbb{A}_{\mathbb{Q}})^{\operatorname{Br}_{\Upsilon,S_{\min}}(C)}$ using our implementation of Algorithm 5.1 is faster than `TwoCoverDescent`, though much of the disparity likely comes down to specifics of the implementation.

Remark 6.1. *We have compared our implementation of Algorithm 5.1 with* `TwoCoverDescent` *in this way for many thousands of curves, finding the outputs to be consistent in all cases when both terminated (i.e., without error, running out of memory, or being interrupted intentionally or otherwise). We take this as strong evidence of the correctness of these algorithms and their implementations in magma.*

6.2. **A genus 50 example.**

Proposition 6.2. *Let $C/\mathbb{Q}$ be the genus 50 hyperelliptic curve defined by $y^2 = 5f(x)$ where*

$$\begin{aligned} f(x) = {} & x^{102} + x^{101} + x^{97} + x^{95} + x^{93} + x^{90} + x^{86} + x^{80} + x^{77} + x^{75} + x^{71} \\ & + x^{70} + x^{68} + x^{65} + x^{64} + x^{63} + x^{62} + x^{59} + x^{58} + x^{53} + x^{50} + x^{49} \\ & + x^{48} + x^{46} + x^{45} + x^{44} + x^{38} + x^{37} + x^{36} + x^{35} + x^{32} + x^{31} + x^{26} \\ & + x^{25} + x^{22} + x^{16} + x^{11} + x^{8} + x^{7} + x + 1\,. \end{aligned}$$

Then $C(\mathbb{A}_\mathbb{Q}) \neq \emptyset$, but $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(C)} = \emptyset$.

Proof of Proposition 6.2. It is straightforward to check with the help of magma that C is locally soluble. Let θ denote a root of $f(x)$. Then $L = \mathbb{Q}[\theta]$ is a degree 102 number field and $\ell = \theta \in L^\times$ is an element of norm $f(0) = 1$. This corresponds to an element $\mathcal{A}_\ell \in \mathrm{Br}_\Upsilon(C)$. We will show that the evaluation maps $\mathcal{A}_\ell : C(\mathbb{Q}_v) \to \mathrm{Br}(\mathbb{Q}_v)$ are constant for all $v \in \Omega_\mathbb{Q}$ and are trivial if and only if $v \neq 5$. It follows that $C(\mathbb{A}_\mathbb{Q})^{\mathcal{A}_\ell} = \emptyset$. In effect we are running Algorithm 5.1 with input $\ell_1 = \ell = \theta$.

For all odd primes v, the valuation of the discriminant of $f(x)$ is at most 1. So as in the proof of Lemma 4.11 the evaluation maps are trivial for $v \notin \{2, 5, \infty\}$. To determine the evaluation map at $v = \infty$, we check that $f(x)$ has two real roots $r_1 \leq r_2 \in \mathbb{R}$, so $C(\mathbb{R})$ is a single component whose image in $\mathbb{P}^1(\mathbb{R})$ is the complement of the interval (r_1, r_2). Since the evaluation map is locally constant, it is constant. Taking $P \in C(\mathbb{R})$ with $x(P) = a > r_2$ we have $\mathrm{inv}_\infty(\mathcal{A}_\ell(P)) = (x(P) - r_1, r_1)_\mathbb{R} + (x(P) - r_2, r_2)_\mathbb{R}$ by Lemma 4.10. Both terms in this sum are trivial because $x(P) - r_i > 0$ for $i = 1, 2$.

The polynomial $f(x)$ has a single 5-adic root $r \in \mathbb{Q}_5$ and it is a unit congruent to 3 mod 5. Using the algorithm of [BS09, Section 4] one checks that $\mu_5 : C(\mathbb{Q}_5) \to L_5^\times/\mathbb{Q}_5^\times L_5^{\times 2}$ is constant (because all 5-adic points lie in a small neighborhood of the point $Q = (r, 0)$). Write $5f(x) = (x - r)\tilde{f}(x)$ and let $\theta_1, \ldots, \theta_n \in L_5 = \mathbb{Q}_5 \times \mathbb{Q}_5(\theta_1) \times \cdots \times \mathbb{Q}_5(\theta_n)$ be roots of the irreducible factors of $\tilde{f}$. Using Lemma 4.10 we have $\mathrm{inv}_5(\mathcal{A}_\ell(Q)) = (r, \tilde{f}(r))_{\mathbb{Q}_5} + \Sigma_{\theta_i \neq r}(\theta_i, r - \theta_i)_{\mathbb{Q}_5(\theta_i)}$. The terms $(\theta_i, r - \theta_i)$ are all 0 because 5 does not divide the discriminant of $f(x)$ and this implies that any root or difference of two roots must have even valuation. On the other hand, $r \in \mathbb{Z}_5^\times$ is not a square and $\tilde{f}(r) \in 5\mathbb{Z}_5^\times$, so $(r, \tilde{f}(r))_{\mathbb{Q}_5} = 1/2$.

Using the algorithm of [BS09, Section 4] we compute that $\mu_2 : C(\mathbb{Q}_2) \to L_2^\times/\mathbb{Q}_2^\times L_2^{\times 2}$ has image equal to the classes represented by $4 - \theta$, and $1/a - \theta$ for $a \in \{4, 12, 20, 28\}$. As above, Lemma 4.10 reduces checking that $\mathcal{A}_\ell(C(\mathbb{Q}_2)) = 0 \in \mathrm{Br}(\mathbb{Q}_2)$ to the computation of Hilbert symbols of these values with $\ell = \theta$ at the primes of L above 2. □

Let us make some further remarks on the example in Proposition 6.2. The Galois group of $f(x)$ is the full symmetric group so computation of class and unit group of the number field it defines are completely out of reach even assuming GRH. Second, the Jacobian J of the curve is absolutely simple and $\mathrm{End}(J) = \mathbb{Z}$ (one checks that $J_{\mathbb{F}_3}$ and $J_{\mathbb{F}_7}$ are both absolutely simple and their endomorphism algebras are linearly disjoint over $\mathbb{Q}$ by computing zeta functions),

so there are no maps to lower positive genus curves or isogenies of degree a small power of 2 that might be used to disprove the existence of rational points on C.

The curve was selected as follows. We wanted a polynomial with equal leading and constant coefficients, so that a root gives an element of norm 1 and thus a Brauer class on the curve which might yield an obstruction to the Hasse principle. To carry out the required computations we must be able to factor the discriminant of the polynomial and compute Hilbert symbols in the completions of the number field it defines. Even the latter becomes rather expensive when there are 2-adic primes of large degree (though a better implementation could likely improve upon this). For this reason we generated $f(x)$ as a product of minimal polynomials of random elements of $\mathbb{F}_{2^8}$. The curve defined by $f(x)$ has rational points above $0, \infty \in \mathbb{P}^1(\mathbb{Q})$, so we considered quadratic twists. The quadratic twists by $d = -1, 2, 3$ are not locally soluble, but the twist by $d = 5$ is.

We carried out similar computations for other polynomials of similar degree with a norm 1 root and found that the root gives an obstruction with reasonable frequency (at least for these high genus curves).

6.3. **Statistics from random samples.** To test the effectiveness of our algorithm, we attempted to decide on the existence of rational points on several large random samples of hyperelliptic curves over $\mathbb{Q}$. In this subsection we report on the results.

For various values of g and n we drew samples from the set $M(g, n)$ of genus g hyperelliptic curves over $\mathbb{Q}$ defined by $y^2 = f(x)$, where $f(x) = f_{2g+2}x^{2g+2} + \ldots + f_0 \in \mathbb{Z}[x]$ is an irreducible polynomial of degree $2g+2$, and $|f_i| \leq n$ for $i = 0, \ldots, 2g+2$. Samples were drawn by choosing the coefficients uniformly at random. Each curve C is classified as one of the following cases:

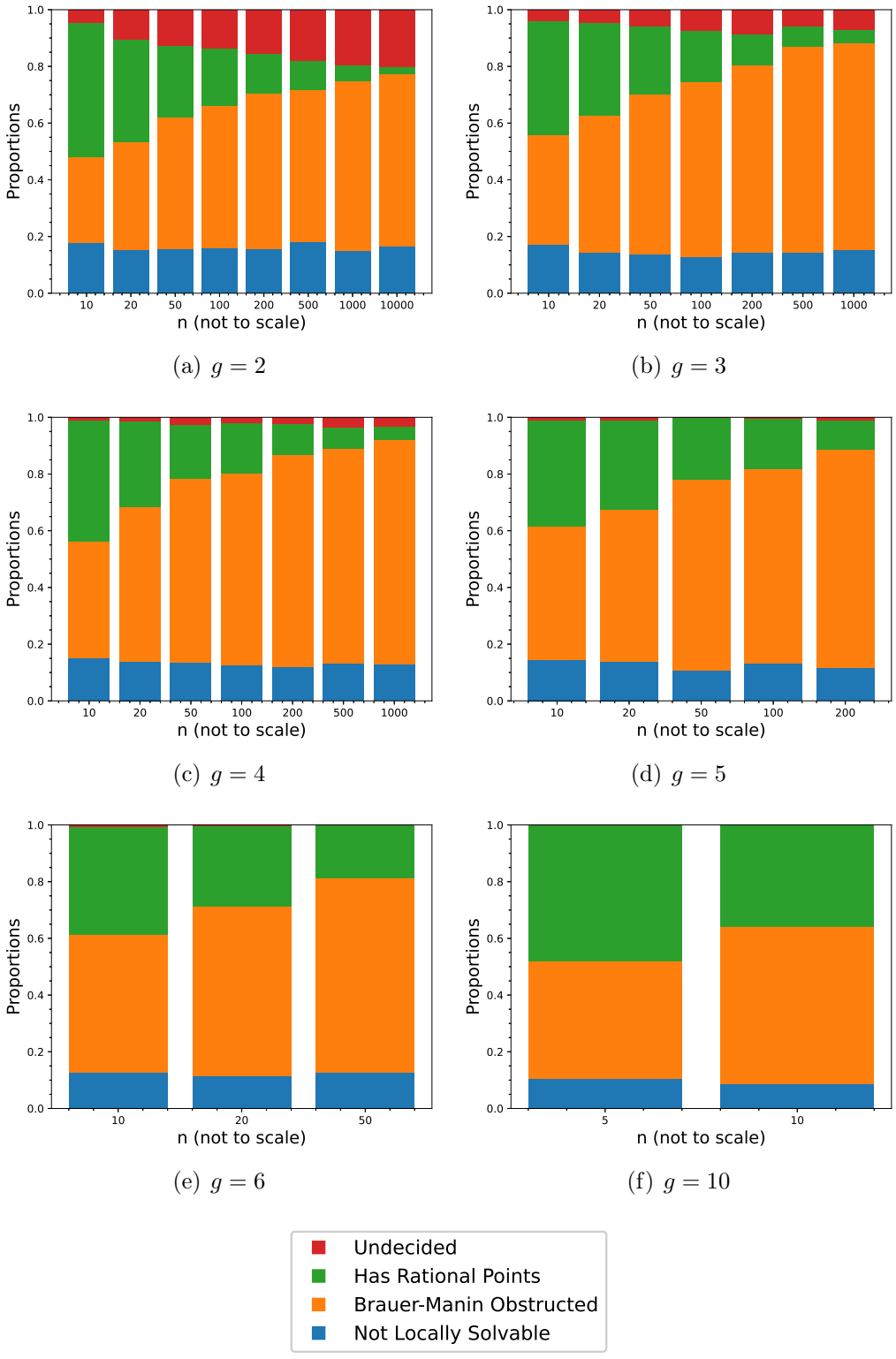
(1) **Not Locally Soluble**; $C(\mathbb{A}_\mathbb{Q}) = \emptyset$.
(2) **Brauer-Manin Obstructed**; $C(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ and $C(\mathbb{A}_\mathbb{Q})^B = \emptyset$ for B a subset of $\mathrm{Br}_{\Upsilon,S}(C)$ such that $C(\mathbb{A}_\mathbb{Q})^B = C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}_{\Upsilon,S}(C)}$ conditionally on GRH and S is the set including all primes of $S_{\min}$, all primes up to 10^3 and all primes of bad reduction up to 10^4.
(3) **Has a Rational Point**; C has a rational point whose x-coordinate is of height $\leq 10^6$
(4) **Undecided**; C does not fall into one of the categories above.

Note that in cases (1) - (3) the existence of rational points on C has been decided.

The graphs and tables below give the proportion of curves in each case, in each of our samples. Sample sizes for each (g, n) ranged from 500 to 2000.

The data allows for a few interesting observations:

- For each g the proportion of curves that are not locally soluble appears to remain stable as n varies.
- The vast majority of of hyperelliptic curves have a Brauer-Manin obstruction to the existence of rational points which we are able to compute using Algorithm 5.1.
- The proportion of curves with a Brauer-Manin obstruction appears to increase with both g and n. The dependence on g is in line with the results of [Bha13]. For curves of genus ≥ 5 we are able to decide existence of rational points for over 99% of curves.
- The proportion of undecided curves appears to decrease as the genus increases, but increases slightly as n is increased.



(a) $g = 2$ (b) $g = 3$

(c) $g = 4$ (d) $g = 5$

(e) $g = 6$ (f) $g = 10$

FIGURE 1. Statistics on random samples of genus g and coefficient bound n

g	n	$C(\mathbb{Q}) \neq \emptyset$	$C(\mathbb{A}_{\mathbb{Q}})^B = \emptyset$		Undecided
			$C(\mathbb{A}_{\mathbb{Q}}) = \emptyset$	$C(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$	
2	10	47.3%	17.8%	30.3%	4.6%
	20	36.2%	15.2%	38.3%	10.3%
	50	25.5%	15.5%	46.4%	12.6%
	100	20.3%	15.8%	50.4%	13.5%
	200	14%	15.6%	54.9%	15.5%
	500	10.3%	18%	53.8%	17.9%
	1000	5.6%	15.1%	59.7%	19.6%
	10000	2.7%	16.6%	60.7%	20%
3	10	40.1%	17.1%	38.8%	4%
	20	32.9%	14.2%	48.5%	4.4%
	50	24.2%	13.9%	56.1%	5.8%
	100	18.2%	12.7%	61.9%	7.2%
	200	11%	14.4%	66.0%	8.6%
	500	7.1%	14.3%	72.7%	5.9%
	1000	4.8%	15.1%	73.2%	6.9%
4	10	42.6%	15.2%	41%	1.2%
	20	30.2%	13.8%	54.6%	1.4%
	50	19.2%	13.6%	64.6%	2.6%
	100	17.8%	12.6%	67.6%	2%
	200	10.8%	12%	74.8%	2.4%
	500	7.4%	13.2%	75.8%	3.6%
	1000	4.4%	13%	79.2%	3.4%
5	10	37.4%	14.4%	47.2%	1%
	20	31.6%	13.8%	53.6%	1%
	50	21.6%	10.8%	67.4%	0.2%
	100	18%	13.2%	68.4%	0.4%
	200	10.2%	11.8%	76.8%	1.2%
6	10	37.8%	12.7%	48.7%	0.8%
	20	28.4%	11.4%	59.8%	0.4%
	50	18.5%	12.5%	68.8%	0.2%
10	5	48.2%	10.4%	41.4%	0%
	10	36%	8.8%	55.2%	0%

TABLE 1. Statistics on random samples of genus g and coefficient bound n

REFERENCES

[Ant11] Marco Antei, *On the abelian fundamental group scheme of a family of varieties*, Israel J. Math. **186** (2011), 427–446, DOI 10.1007/s11856-011-0147-9. ↑5

[Bha13] Manjul Bhargava, *Most hyperelliptic curves over Q have no rational points* (2013), available at arXiv:1308.0395. ↑1, 20

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). ↑1

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), Paper No. e6, 80, DOI 10.1017/fms.2016.1. ↑2

[BF05] Nils Bruin and E. Victor Flynn, *Towers of 2-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347, DOI 10.1090/S0002-9947-05-03954-1. ↑2

[BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8. ↑2, 3, 4, 5, 10, 12, 13, 15, 16, 17, 18, 19

[BS10] Nils Bruin and Michael Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, DOI 10.1112/S1461157009000187. ↑3

[Čes15] Kęstutis Česnavičius, *Poitou-Tate without restrictions on the order*, Math. Res. Lett. **22** (2015), no. 6, 1621–1666, DOI 10.4310/MRL.2015.v22.n6.a5. ↑6, 7

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). ↑3

[CTS87] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *La descente sur les variétés rationnelles. II*, Duke Math. J. **54** (1987), no. 2, 375–492, DOI 10.1215/S0012-7094-87-05420-2 (French). ↑2

[Cre12] Brendan Creutz, *A Grunwald-Wang type theorem for abelian varieties*, Acta Arith. **154** (2012), no. 4, 353–370, DOI 10.4064/aa154-4-2. ↑6

[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. ↑3

[Cre20] Brendan Creutz, *Generalized Jacobians and explicit descents*, Math. Comp. **89** (2020), no. 323, 1365–1394, DOI 10.1090/mcom/3491. ↑2, 9, 10, 13

[CV15] Brendan Creutz and Bianca Viray, *Two torsion in the Brauer group of a hyperelliptic curve*, Manuscripta Math. **147** (2015), no. 1-2, 139–167, DOI 10.1007/s00229-014-0721-7. ↑2, 3, 8, 9, 13, 14

[Fly04] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466, DOI 10.1007/s00229-004-0502-9. ↑3

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. ↑11

[Mil06] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006. ↑3, 4

[Poo06] Bjorn Poonen, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. ↑1

[Poo17] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. ↑4

[Poo21] Bjorn Poonen, *A p-adic approach to rational points on curves*, Bull. Amer. Math. Soc. (N.S.) **58** (2021), no. 1, 45–56, DOI 10.1090/bull/1707. ↑3

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. ↑2, 5, 10, 17

[Sch99] Victor Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–University of Michigan. ↑3

[Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. ↑1, 2, 4, 5, 6, 8, 10, 12

[Sto07] Michael Stoll, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391, DOI 10.2140/ant.2007.1.349. ↑1