Heuristics for the Brauer–Manin Obstruction for Curves

Bjorn Poonen

CONTENTS

We conjecture that if C is a curve of genus > 1 over a number field k such that $C(k) = \varnothing$, then a method of Scharaschkin (essentially equivalent to the Brauer–Manin obstruction in the context of curves) supplies a proof that $C(k) = \varnothing$. As evidence, we prove a corresponding statement in which $C(\mathbb{F}_v)$ is replaced by a random subset of the same size in $J(\mathbb{F}_v)$ for each residue field $\mathbb{F}_v$ at a place v of good reduction for C, and the orders of Jacobians over finite fields are assumed to be smooth (in the sense of having only small prime divisors) as often as random integers of the same size. If our conjecture holds, and if Tate–Shafarevich groups are finite, then there exists an algorithm to decide whether a curve over k has a k-point, and the Brauer–Manin obstruction to the Hasse principle for curves over the number fields is the only one.

1. SETUP

Let k be a number field. Fix an algebraic closure $\overline{k}$ of k, and let $G = \mathrm{Gal}(\overline{k}/k)$. Let C be a curve of genus g over k. (In this paper, curves are assumed to be smooth, projective, and geometrically integral.) Let $\overline{C} = C \times_k \overline{k}$. Let J be the Jacobian of C, which is an abelian variety of dimension g over k. Assume that $\overline{C}$ has a G-invariant line bundle of degree 1: this gives rise to a k-morphism $C \to J$, and it is an embedding if $g > 0$. Let S_C be the set of finite primes v of good reduction for C. Similarly define S_A for any abelian variety A over k. We have $S_C \subseteq S_J$.

2. DETERMINING THE SET OF RATIONAL POINTS

Suppose that generators of the Mordell–Weil group $J(k)$ are known. Then $C(k)$ equals the set of points in $J(k)$ that lie on the subvariety C. We would like to know whether $C(k)$ can be calculated, especially in the case $g > 1$ in which $C(k)$ is guaranteed to be finite by [Faltings 83].

If $J(k)$ is finite, then in principle we can list its elements and check which of them lie on C. On the other

2000 AMS Subject Classification: Primary 11G30; Secondary 11G10, 14G05

Keywords: Chabauty, Jacobian, Brauer–Manin obstruction, Hasse principle

1058-6458/2006 $0.50 per page
Experimental Mathematics **15**:4, page 415

hand, if $J(k)$ is infinite, it can be very difficult to decide which points of $J(k)$ lie on C.

3. CHABAUTY'S APPROACH

One approach, due to C. Chabauty [Chabauty 41], works in $J(k_v)$, where k_v is the completion of k at a nonarchimedean place v. Chabauty observed that the closure $\overline{J(k)}$ of $J(k)$ in $J(k_v)$ is an analytic submanifold of $J(k_v)$, and proved that *if the rank of $J(k)$ is less than g*, the subset of points in $\overline{J(k)}$ lying on C is finite; in this case, as explained by R. Coleman [Coleman 85], one gets an effective upper bound for $\#C(k)$. Often one can even determine $C(k)$ explicitly. But the dimension hypothesis is not always satisfied, and even when it is, the upper bound on $\#C(k)$ may fail to be sharp.

4. SCHARASCHKIN'S APPROACH

A more recent approach, suggested by V. Scharaschkin [Scharaschkin 04], tries to find which points of $J(k)$ lie on C modulo $\mathfrak{p}$ for many primes $\mathfrak{p}$. More precisely, he proposes the following method for proving that $C(k)$ is empty. Choose a finite subset $S \subset S_C$. Let $\mathbb{F}_v$ be the residue field at v. Then we have a commutative square

$$\begin{array}{ccc} C(k) & \dashrightarrow & \prod_{v\in S} C(\mathbb{F}_v) \\ \downarrow & & \downarrow \\ J(k) & \longrightarrow & \prod_{v\in S} J(\mathbb{F}_v)\ . \end{array}$$

If the images of the solid arrows in $\prod_{v\in S} J(\mathbb{F}_v)$ do not intersect, then $C(k)$ is empty.

Remark 4.1. For this paragraph we assume that the Tate–Shafarevich group $Ш(J)$ is finite, or at least that its maximal divisible subgroup is trivial. Scharaschkin [Scharaschkin 04] proved that then the potential obstruction to the existence of k-points described above is part of the Brauer–Manin obstruction. More precisely, he showed that if we consider the product of $J(k_v)$ (modulo its connected component if v is archimedean) over all places v instead of a product of only $J(\mathbb{F}_v)$ over only places of good reduction, then we recover exactly the Brauer–Manin obstruction.

For the connection of the Brauer–Manin obstruction to the information on rational points obtained from finite étale covers, see [Stoll 05].

5. A CONJECTURE AND ITS IMPLICATIONS

We conjecture the following, based on heuristics to be explained later.

Conjecture 5.1. *Let $C \to J$ be as in Section 1, with $g > 1$. If $C(k) = \varnothing$, then there exists a finite subset $S \subset S_C$ 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.*

The importance of Conjecture 5.1 is given by the following result:

Theorem 5.2. *Assume Conjecture 5.1. Assume also that Tate–Shafarevich groups of Jacobians of curves over number fields are finite. Then*

(a) *There is an algorithm that takes as input a number field k and a curve C over k, and decides whether C has a k-point.*

(b) *The Brauer–Manin obstruction to the Hasse principle is the only obstruction to the existence of a k-point on a curve C over a number field k.*

Proof: For details on how elements of k and curves over k can be represented, see [Baker et al. 05, Section 5.1].

Before proceeding, we recall a few well-known facts:

(i) There exists an algorithm for deciding whether a smooth projective variety X over k has a point over every completion k_v. (Sketch of proof: For all nonarchimedean primes v of sufficiently large norm, the Weil conjectures and Hensel's lemma imply that X automatically has a k_v-point. One can test the remaining v individually, again using Hensel's lemma in the nonarchimedean case.)

(ii) If X is a torsor of an abelian variety A over a number field k, and if $Ш(A)$ is finite, then there exists an algorithm to decide whether X has a k-point, and the Brauer–Manin obstruction to the Hasse principle is the only one for X. (Sketch of proof: By the previous fact, we may assume $X(k_v) \neq \varnothing$ for all v, so X represents an element of $Ш(A)$. If we search for k-points on X by day, and perform higher and higher descents on A by night, we will eventually decide whether X has a k-point, assuming the finiteness of $Ш(A)$, even if we are not given a bound on $\#Ш(A)$. It remains to show that if X has no k-point, then there is a Brauer–Manin obstruction. Under our assumption

that Ш(A) is finite, the Cassels–Tate pairing

$$\langle\ ,\ \rangle\colon Ш(A) \times Ш(A^\vee) \to \mathbb{Q}/\mathbb{Z}$$

is nondegenerate. If X has no k-point, then X corresponds to a nonzero element of Ш(A), so there is a torsor Y of the dual abelian variety $A^\vee$ such that $\langle X, Y\rangle \neq 0$. By [Manin 71, Theorem 6], there is an element $y \in \operatorname{Br} X$ related to Y such that the Brauer pairing of y with every adelic point on X gives the value $\langle X, Y\rangle \neq 0$, so X has a Brauer–Manin obstruction.)

(iii) There exists an algorithm that in principle, given any abelian variety A over k such that Ш(A) is finite, computes a finite list of generators of $A(k)$. (Sketch of proof: Compute the 2-Selmer group Sel of A. Using (ii), we can decide which of its elements map to 0 in Ш(A), and hence determine the image of $A(k)/2A(k) \to$ Sel. Search for points in $A(k)$ until one has enough to generate the image of $A(k)/2A(k) \to$ Sel. Then the usual proof of the Mordell–Weil theorem given the weak Mordell–Weil theorem (see [Serre 97, Section 4.4], for example) bounds the heights of generators of $A(k)$. Finally, search to find all points of height up to that bound.)

We now return to our problem. By [Baker et al. 05, Lemma 5.1(1)], we can compute the genus g of C, so we may break into cases according to the value of g.

If $g = 0$, then C satisfies the Hasse principle. Thus to test for the existence of a k-point, it suffices to use fact (i) above.

If $g = 1$, then C is a torsor of its Jacobian J, so it suffices to use (ii).

From now on, we suppose $g \geq 2$. By (i), we may reduce to the case that $C(k_v)$ is nonempty for every v. Let $X := \mathbf{Pic}^1_{C/k}$ be the variety parameterizing degree-1 line bundles on C. Thus X is a torsor of the Jacobian J. We have a canonical injection from C to X taking a point $c \in C$ to the class of the associated degree-1 divisor. By (ii), we can check whether X has a k-point; if not, then C has no k-point, and there is a Brauer–Manin obstruction for X, which pulls back to a Brauer–Manin obstruction for C. Thus from now on, we may assume that X has a k-point. In other words, $\overline{C}$ has a G-invariant line bundle of degree 1. Such a G-invariant line bundle can be found by a search, and it allows us to identify X with J. We now can search for k-points on C each day, while running Scharaschkin's method using the first r primes in S_C for larger and larger r each night, making use of the generators of $J(k)$ computed as in (iii). Conjecture 5.1 implies that one of these two processes will terminate. Thus there exists an algorithm for deciding whether C has a k-point. Moreover, as mentioned in Remark 4.1, assuming finiteness of Ш(J), if Scharaschkin's method proves the nonexistence of k-points, then there is a Brauer–Manin obstruction. □

Remark 5.3. If one knows that the Brauer–Manin obstruction to the Hasse principle is the only one for a smooth projective variety X, that in itself lets one determine whether X has a k-point, in principle, as we will explain in the following paragraph. This gives an alternative approach to Theorem 5.2(a), based on part (b).

By an unpublished result of O. Gabber, re-proved by A. J. de Jong, each element of the cohomological Brauer group $\operatorname{Br} X := H^2_{\text{et}}(X, \mathbb{G}_m)$ can be represented by an Azumaya algebra $\mathcal{A}$, i.e., a locally free $\mathcal{O}_X$-algebra that is étale locally isomorphic to a finite-dimensional matrix algebra. Each $\mathcal{A}$ can be described by a finite amount of data:

1. a covering of X by finitely many Zariski-open subsets X_i such that $\mathcal{A}|_{X_i}$ is free as an $\mathcal{O}_{X_i}$-module,
2. the multiplication table for $\mathcal{A}|_{X_i}$ with respect to a chosen $\mathcal{O}_{X_i}$-basis, for each i,
3. the change-of-basis map on the intersection $X_i \cap X_j$, for each i and j,
4. a covering $U_i \to X_i$ in the étale topology, for each i,
5. a positive integer r_i and an $\mathcal{O}_{U_i}$-algebra isomorphism $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \simeq M_{r_i}(\mathcal{O}_{U_i})$, for each i.

Moreover, given such data, one can easily check whether it actually defines an Azumaya algebra. Therefore there is a (very inefficient) algorithm that when left running forever, eventually produces all Azumaya algebras over X, each possibly occurring more than once, simply by enumerating and checking each possible set of data. Now, we search for k-points by day and generate Azumaya algebras by night, calculating at the end of each night whether the Azumaya algebras generated so far give an obstruction.

Remark 5.4. It is not clear whether Conjecture 5.1 and the finiteness of Tate–Shafarevich groups imply the existence of an algorithm for *listing* all k-points on a given curve C of genus $g \geq 2$ over k. For the listing problem, applying Chabauty's method to finite étale covers

seems more promising; see [Stoll 05] for an analysis of the situation.

6. COMPUTATIONAL EVIDENCE FOR THE CONJECTURE

E. V. Flynn [Flynn 04] has developed an implementation of Scharaschkin's method for genus-2 curves over $\mathbb{Q}$. He tested 145 such curves defined by equations with small integer coefficients, having $\mathbb{Q}_p$-points for all $p \leq \infty$, but having no $\mathbb{Q}$-point with x-coordinate of height less than 10^{30}. These were grouped according to the rank r of the Jacobian. In all cases with $r \leq 1$, he successfully showed that there was a Brauer–Manin obstruction. In most cases with $r = 2$, a Brauer–Manin obstruction was found, and all the unresolved $r = 2$ cases were later resolved by an improved implementation of M. Stoll. The remaining cases had $r = 3$, and a few of these were resolved; it was unclear from the computation whether the remaining ones could be resolved by a longer computation: the combinatorics quickly became prohibitive.

7. THEORETICAL EVIDENCE FOR THE CONJECTURE

Here we give a heuristic analysis of Conjecture 5.1. Recall that if $B \in \mathbb{R}_{>0}$, an integer is called *B-smooth* if all its prime factors are less than or equal to B. For any fixed $u \in (0,1)$, the fraction of integers in $[1,B]$ that are B^u-smooth tends to a positive constant as $B \to \infty$ [De Bruijn 51].

As our main evidence for Conjecture 5.1, we prove a modified version of it in which $C(\mathbb{F}_v)$ is modeled by a random subset of $J(\mathbb{F}_v)$ of the same order, and in which we assume that the integer $\#J(\mathbb{F}_v)$ is as smooth as often as a typical integer of its size. The smoothness assumption is formalized in the following:

Conjecture 7.1. *Let A be an abelian variety over a number field k, and let $u \in (0,1)$. Then*

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

Let $g = \dim A$. If $\#A(\mathbb{F}_v)$ behaves like a typical integer of its size, which is about $(\#\mathbb{F}_v)^g \leq B^g$, then it should have a positive probability of being B^u-smooth, since B^u is a constant power of B^g. If anything, $\#A(\mathbb{F}_v)$ can be expected to factor more than typical integers its size, because of splitting of A up to isogeny, or because of biases in the probability of being divisible by small primes. Thus Conjecture 7.1 is reasonable.

We are now ready to state our main result giving evidence for Conjecture 5.1.

Theorem 7.2. *Let $C \to J$ be as in Section 1, with $g > 1$. Assume Conjecture 7.1 for J. For each prime $v \in S_C$, let $\mathcal{C}(\mathbb{F}_v)$ be a random subset of $J(\mathbb{F}_v)$ of size $\#C(\mathbb{F}_v)$; we assume that the choices for different v are independent. Then with probability* 1*, there exists a finite subset $S \subseteq S_C$ such that the images of $J(k)$ and $\prod_{v\in S} \mathcal{C}(\mathbb{F}_v)$ in $\prod_{v\in S} J(\mathbb{F}_v)$ do not intersect.*

Proof: It suffices to find S such that the probability that the images intersect is arbitrarily small.

Given $B > 0$, let $S = S(B)$ be the set of $v \in S_C$ such that $\#\mathbb{F}_v \leq B^2$ and $\#J(\mathbb{F}_v)$ is B-smooth. Because we have assumed Conjecture 7.1 for J, there exists $c > 0$ such that for arbitrarily large $B \in \mathbb{R}_{>0}$ (the square root of the B occurring in Conjecture 7.1), the set S contains at least a fraction c of the primes $v \in S_C$ with $\#\mathbb{F}_v \leq B^2$.

Let $\pi(x)$ be the number of rational primes less than or equal to x. The prime number theorem says that $\pi(x) = (1 + o(1))x/\log x$ as $x \to \infty$. For $v \in S$, the Weil conjectures give $\#J(\mathbb{F}_v) \leq O\left((\#\mathbb{F}_v)^{2g}\right) \leq B^{2g+o(1)}$ as $B \to \infty$, so by B-smoothness, the least common multiple L of $\#J(\mathbb{F}_v)$ for $v \in S$ satisfies

$$L \leq \prod_{\text{primes } p \leq B} p^{\left\lfloor \log_p B^{2g+o(1)} \right\rfloor} \leq \prod_{\text{primes } p \leq B} B^{2g+o(1)},$$

or equivalently,

$$\log L \leq \pi(B)(2g + o(1)) \log B = (2g + o(1))B.$$

Suppose that $J(k)$ is generated by r elements. Every element of $\prod_{v\in S} J(\mathbb{F}_v)$ has order dividing L, so the order of the image I of $J(k)$ in $\prod_{v\in S} J(\mathbb{F}_v)$ is at most

$$L^r \leq \exp\left((2g + o(1))rB\right).$$

The probability that a fixed element of a set of size n belongs to a random subset of size m is m/n, so the probability P that a fixed element of I belongs to the image I' of $\prod_{v\in S} \mathcal{C}(\mathbb{F}_v) \to \prod_{v\in S} J(\mathbb{F}_v)$ satisfies

$$P = \prod_{v\in S} \frac{\#C(\mathbb{F}_v)}{\#J(\mathbb{F}_v)} \leq \prod_{v\in S} \frac{(\#\mathbb{F}_v)^{1+o(1)}}{(\#\mathbb{F}_v)^{g+o(1)}},$$

where again we have used the Weil conjectures. Equivalently,

$$\log P \leq (1 - g + o(1)) \sum_{v\in S} \log \#\mathbb{F}_v.$$

The number of primes v of k with $\#\mathbb{F}_v \le B^2$ is at least the number of rational primes $p \le B^2$ that split completely in k, which is asymptotically greater than or equal to $c_1\pi(B^2)$. (We use $c_1, c_2, \dots$ to denote positive constants independent of B.) Since S contains a positive fraction of these v, and since the numbers $\#\mathbb{F}_v$ are powers of primes, with each prime occurring at most $[k:\mathbb{Q}]$ times, we find that $\sum_{v\in S} \log \#\mathbb{F}_v$ is at least the sum of $\log p$ for the first $c_2\pi(B^2)$ primes. By the prime number theorem, the nth prime is $(1+o(1))n\log n$, so

$$\begin{aligned}\sum_{v\in S} \log \#\mathbb{F}_v &\ge \sum_{n=1}^{c_2\pi(B^2)} \log((1+o(1))n\log n)\\ &\ge \sum_{n=c_2\pi(B^2)/2}^{c_2\pi(B^2)} \log((1+o(1))n\log n)\\ &\ge c_3\pi(B^2)\log\pi(B^2)\\ &\ge c_4 B^2\end{aligned}$$

as $B\to\infty$. Since $1-g<0$, we get

$$\log P \le -c_5 B^2,$$

or equivalently,

$$P \le \exp(-c_5 B^2).$$

Thus the probability that I intersects I' is at most

$$\#I \cdot P \le \exp\left((2g+o(1))rB\right)\cdot\exp(-c_5B^2),$$

which tends to 0 as $B\to\infty$, as desired. □

Remark 7.3. For the case of $C(k)$ nonempty, we would have liked to analyze a refined heuristic that reflects the existence of the k-points. Namely, suppose that $\mathcal{C}(\mathbb{F}_v)$ is a random subset of $J(\mathbb{F}_v)$ of size $\#C(\mathbb{F}_v)$ chosen *subject to the constraint that it contains the image of* $C(k)$ *in* $J(\mathbb{F}_v)$. We then expect that with probability 1, the only points of $J(k)$ whose image in $\prod_{v\in S_C} J(\mathbb{F}_v)$ lies in the image of $\prod_{v\in S_C}\mathcal{C}(\mathbb{F}_v)$ are those in $C(k)$. But we were unable to prove this, even assuming Conjecture 7.1.

Question 7.4. Is it true more generally that if X is a closed subvariety of an abelian variety A over a number field k, and S is a density-1 set of primes of good reduction for X and A, then the intersection of the closure of the image of $A(k)$ in $\prod_{v\in S} A(\mathbb{F}_v)$ with $\prod_{v\in S} X(\mathbb{F}_v)$ equals the closure of the image of $X(k)$ in $\prod_{v\in S} A(\mathbb{F}_v)$? One could also ask the question with $\prod_{v\in S} A(\mathbb{F}_v)$ replaced by the product of $A(k_v)$ (modulo its connected component) over all v. We expect a positive answer; this together with finiteness of Ш(A) would imply that the Brauer–Manin obstruction to the Hasse principle is the only one for such X; cf. Remark 4.1.

ACKNOWLEDGMENTS

I thank Jean-Louis Colliot-Thélène and Michael Stoll for several discussions about the Brauer–Manin obstruction during the Fall 2004 trimester at the Institut Henri Poincaré. I thank the Institut Henri Poincaré and the Isaac Newton Institute for their hospitality. This research was supported by NSF grant DMS-0301280 and a Packard Fellowship.

REFERENCES

[Baker et al. 05] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. "Finiteness Results for Modular Curves of Genus at Least 2." *Amer. J. Math.* 127 (2005), 1325–1387.

[Chabauty 41] Claude Chabauty. "Sur les points rationnels des courbes algébriques de genre supérieur à l'unité." *C. R. Acad. Sci. Paris* 212 (1941), 882–885.

[Coleman 85] Robert F. Coleman. "Effective Chabauty." *Duke Math. J.* 52:3 (1985), 765–770.

[De Bruijn 51] N. G. de Bruijn. "On the Number of Positive Integers $\le x$ and Free of Prime Factors $> y$." *Nederl. Acad. Wetensch. Proc. Ser. A.* 54 (1951), 50–60.

[Faltings 83] G. Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern." *Invent. Math.* 73:3 (1983), 349–366. Published in English translation as "Finiteness Theorems for Abelian Varieties over Number Fields." In *Arithmetic Geometry*, pp. 9–27. New York: Springer-Verlag, 1984. Erratum in *Invent. Math.* 75 (1984), 381.

[Flynn 04] E. V. Flynn. "The Hasse Principle and the Brauer–Manin Obstruction for Curves." *Manuscripta Math.* 115:4 (2004), 437–466.

[Manin 71] Y. I. Manin. "Le groupe de Brauer–Grothendieck en géométrie diophantienne." In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pp. 401–411. Paris: Gauthier-Villars, 1971.

[Scharaschkin 04] Victor Scharaschkin. "The Brauer–Manin Obstruction for Curves." Preprint, 2004.

[Serre 97] Jean-Pierre Serre. *Lectures on the Mordell–Weil Theorem*, Aspects of Mathematics, 3. Braunschweig: Vieweg, Braunschweig, 1997.

[Stoll 05] Michael Stoll. "Finite Descent and Rational Points on Curves." Preprint, 2005.

Bjorn Poonen, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
(poonen@math.berkeley.edu)

Received July 16, 2005; accepted February 12, 2006.