Brauer-Manin Obstruction on Hyperelliptic Curves

Duttatrey Nath Srivastava

School of Mathematics and Statistics,
University of Canterbury, New Zealand

26 November 2020

Hyperelliptic Curves

Problem

A Hyperelliptic curve C (of genus $g = 2$) can be defined as

$$C : y^2 = cf(x),$$

$c \in \mathbb{Q}^*$, with $f(x) \in \mathbb{Q}[x]$ a monic, separable polynomial . How can we figure out (definitively) if $C(\mathbb{Q}) = \emptyset$, i.e. it has no rational solutions ?

- Faltings' Theorem[Fal86]: For curves of genus $g \geq 2$, $C(\mathbb{Q})$ is finite.

Checking ELS(ewhere)

- $\mathbb{R} = \mathbb{Q}_\infty$: Completion of $\mathbb{Q}$ wrt metric $d(x, y) := |x - y|$.
- $\mathbb{Q}_p$: Completion of $\mathbb{Q}$ wrt metric

$$\nu_p(x, y) := p^{-a}$$

  where $a :=$ largest power of prime p dividing $(x - y)$
- $\mathbb{Q}$ can be embedded into $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p.
- Proving that no solution exists over $\mathbb{Q}_p$ for even one prime p means no rational solutions can exist.

Local and Global Solutions

- Checking for Local Solutions is relatively easier than directly searching for Global solutions.
- We thus check for solution on a reasonable subset of $\prod_{p\leq\infty}\mathbb{Q}_p$ (include $p=\infty$ as well), namely the set of Adelic points $\mathbb{A}_{\mathbb{Q}}$.

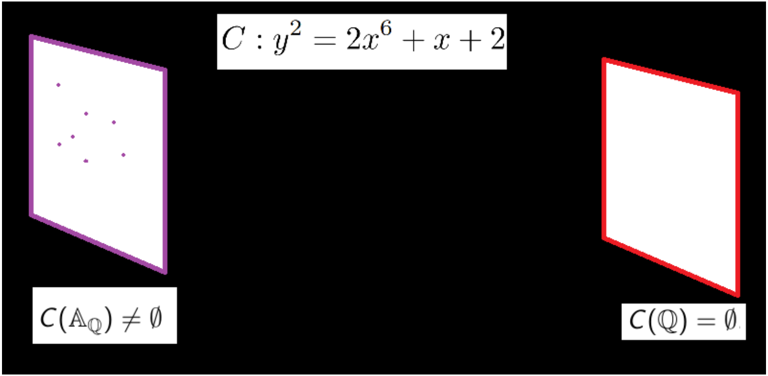
Definition (Adelic Points on Rationals)

The set of adelic points on rationals is defined as

$$\mathbb{A}_{\mathbb{Q}} := \{(x_p)_p \in \prod_{p\leq\infty}\mathbb{Q}_p : x_p \in \mathbb{Z}_p \text{ for all but finitely many primes } p\}$$

.

- Hasse principle : $C(\mathbb{A}_{\mathbb{Q}}) = \emptyset \implies C(\mathbb{Q}) = \emptyset$?
- Hasse Principle holds for curves of genus 0 or 1 but fails for genus 2 or higher.



Brauer Sets

Theorem

For the Brauer sets defined as above and subsets B_1 and B_2 of Br C such that $B_1 \subseteq B_2$, the following series of inclusions holds true:

$$C(\mathbb{Q}) \subseteq C(\mathbb{A}_{\mathbb{Q}})^{B_2} \subseteq C(\mathbb{A}_{\mathbb{Q}})^{B_1} \subseteq C(\mathbb{A}_{\mathbb{Q}}).$$

Let $C(\mathbb{A}_{\mathbb{Q}})$ denote the set of adelic points on C. Given a Brauer class $[\mathcal{A}] \in \text{Br } C$,:

$$\begin{tikzcd}
 & C(\mathbb{Q}) \arrow[r, hook, "inc"] \arrow[d, "\mathcal{A}"] & C(\mathbb{A}_{\mathbb{Q}}) \arrow[d, "\mathcal{A}"] & & \\
0 \arrow[r] & \text{Br}(\mathbb{Q}) \arrow[r, "i"] & \bigoplus_p \text{Br }(\mathbb{Q}_p) \arrow[r, "\sum inv_p"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Definition (Brauer Set)

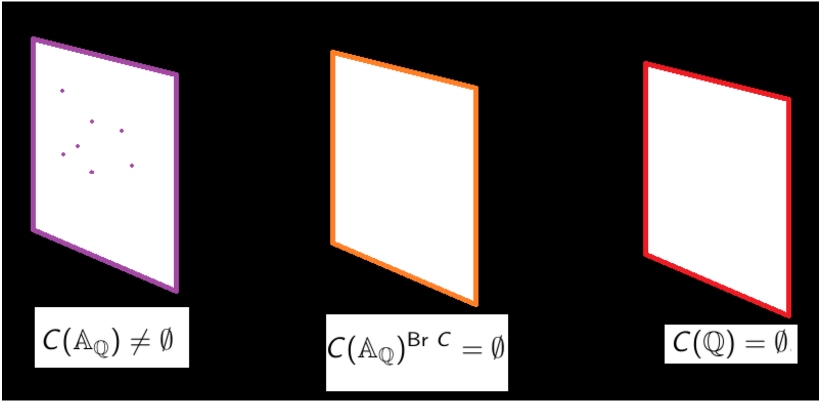
For $B \subseteq \text{Br } C$, Define $C(\mathbb{A}_{\mathbb{Q}})^B := \bigcap_{\mathcal{A} \in B} C(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}}$, where $C(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}} = \{(P_v) \in C(\mathbb{A}_{\mathbb{Q}}) : \sum_v inv_v \mathcal{A}(P_v) = 0\}$ is the Brauer set cut by

Brauer Groups and Adelic Points

Definition

1. The Brauer group $\operatorname{Br} k$ of a field k is the abelian group of equivalence classes of central simple algebras over k, such that $[A].[B] := [A \otimes_k B]$.
2. The Brauer group $\operatorname{Br} C$ of hyperelliptic curve C over k, is the subgroup of $\operatorname{Br}(k(C))$ consisting of all the Brauer classes that admit a covering of C by open subsets U, such that for each $P \in U$ we get a CSA over $k(P)$.

- Every subset (in fact, every element) of the Brauer group describes a subset of Adelic points containing all Rational solutions.



Theory for Computation

Let $C : y^2 = f(x)$ be a hyperelliptic curve. Define $\Phi_\ell : C(\mathbb{A}_\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$ as

$$\Phi_\ell((x_p)_{p\leq\infty}) := \sum_{p\leq\infty} inv_p \mathcal{A}_\ell(x_p)$$

For $\bar{\ell} \in \mathcal{L}_c(S)$, we have $C(\mathbb{A}_\mathbb{Q})^{\gamma(\ell)} = \{x = (x_p) \in C(\mathbb{A}_\mathbb{Q}) : \Phi_\ell(x) = 0\}$

Theorem

Let $S = \{p_1, \ldots, p_n\}$ such that $\mu_p(C(\mathbb{Q}_p))$ is unramified at all $p \notin S$. If for each $W = (W_p)_{p\leq\infty} \in C(\mathbb{A}_\mathbb{Q})$, there is some ℓ_e such that $\Phi_{\ell_e}(W) \neq 0$, then $C(\mathbb{A}_\mathbb{Q})^{\gamma(L_c(S))} = \varnothing$. The converse also holds.

References

Brendan Creutz and Bianca Viray, *Two torsion in the Brauer group of a hyperelliptic curve*, Manuscripta Math. **147** (2015), no. 1-2, 139–167. MR 3336942

Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, pp. 9–26, Springer New York, New York, NY, 1986.

Victor Scharaschkin, *Local -global problems and the brauer-manin obstruction*, Ph.D. thesis, 1999, Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2016-05-20, p. 59.

Michael Stoll, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391. MR 2368954

Brauer Groups and Adelic Points

Definition

1. The Brauer group Br k of a field k is the abelian group of equivalence classes of central simple algebras over k, such that $[A].[B] := [A \otimes_k B]$.
2. The Brauer group Br C of hyperelliptic curve C over k, is the subgroup of Br $(k(C))$ consisting of all the Brauer classes that admit a covering of C by open subsets U, such that for each $P \in U$ we get a CSA over $k(P)$.

Brauer Sets

Let $C(\mathbb{A}_{\mathbb{Q}})$ denote the set of adelic points on C. Given a Brauer class $[\mathcal{A}] \in \mathrm{Br}\ C$,:

$$\begin{tikzcd}
 & C(\mathbb{Q}) \arrow[r, hook, "inc"] \arrow[d, "\mathcal{A}"] & C(\mathbb{A}_{\mathbb{Q}}) \arrow[d, "\mathcal{A}"] & & \\
0 \arrow[r] & \mathrm{Br}(\mathbb{Q}) \arrow[r, "i"] & \bigoplus_p \mathrm{Br}\,(\mathbb{Q}_p) \arrow[r, "\sum inv_p"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Definition (Brauer Set)

Define $C(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}} = \{(P_p) \in C(\mathbb{A}_{\mathbb{Q}}) : \sum_p inv_p \mathcal{A}(P_p) = 0\}$ as the Brauer set cut by the algebra $\mathcal{A}$, and $C(\mathbb{A}_{\mathbb{Q}})^{B} := \bigcap_{\mathcal{A} \in B} C(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}}$ for $B \subseteq \mathrm{Br}\ C$.

2-Torsion in Brauer Groups and γ map

Theorem

For the Brauer sets defined as above, the following series of inclusions holds true:

$$C(\mathbb{Q}) \subseteq C(\mathbb{A}_{\mathbb{Q}})^{Br\ C} \subseteq C(\mathbb{A}_{\mathbb{Q}})^{B} \subseteq C(\mathbb{A}_{\mathbb{Q}}).$$

specifically, it holds for $B = Br\ C[2]$.

In [CV15], the homomorphism

$$\gamma : L^* \to (\mathrm{Br}\ k(C))[2],\ ;\ \ell \mapsto Cor_{k(C_L)/k(C)}((\ell, x-\theta)_2),$$

gives us a subset of Br $C[2]$. (where $L = k[x]/(f(x))$, $Cor_{k(C_L)/k(C)}$ is the corestriction map)

Theorem

Let $\ell \in L^*$. For the curve C as above, $\gamma(\ell) \in Br\ C$ if and only if $N_{L/k}(\ell) \in \langle c \rangle$ where $N_{L/k}$ is the norm on $k-$algebra L.

The image $\gamma(\ell)$ can be written as a tensor product of quaternion algebras over $k(C)$.

Proposition

Suppose $\ell \in L^* \setminus K^*$ *and let* $g(x) \in k[x]$ *be the minimal degree polynomial such that* $g(\alpha) = \ell$. *Set* $r_0 = f(x)$, $r_1 = g(x)$, *and for* $i \geq 0$ *define* r_{i+2} *to be the unique polynomial of degree less than* $\deg(r_{i+1})$ *such that* $r_{i+2} \cong r_i \mod r_{i+1}$. *Then*

$$Cor_{k(C_L)/k(C)}((\ell, x-\alpha)_2) = \left(\bigotimes_{i=0}^{n} (r_{i+1}, r_i)_2\right) \otimes \left(\bigotimes_{i=0}^{n} (a_{i+1}, a_i)_2\right)$$

where a_i *is the leading coefficient of* r_i *and* n *is the first integer such that* $r_{n+2} = 0$.

Our results

- Goal: Compute and understand $\gamma(L_c)$, where $L_c = \{\ell \in L^* : N_{L/k}(\ell) \in \langle c \rangle\}$, and the corresponding obstruction.
- For $k = \mathbb{Q}$, is $\gamma(L_c)$ enough to capture the obstruction coming from Br $C[2]$?
- Issue: L_c is infinite set. Consider $\mathcal{L}_c := \{\overline{\ell} \in L^*/\mathbb{Q}^* L^{*2} : \ell \in L_c\}$. Then $\mathcal{L}_c = \bigcup_S \mathcal{L}_c(S)$ for S finite sets of primes.
- It is enough to consider representatives of $\mathcal{L}_c(S)$ in L_c, which will be in corresponding $L_c(S)$.
- Checking if the obstruction comes from $\gamma(L_c(S))$ is the next task.

Problem

Describe a finite set of primes S such that $C(\mathbb{A}_{\mathbb{Q}})^{\gamma(L_c(S))} = \varnothing$.

Steps required

1. (Global step) Explicitly choosing representatives for distinct elements of $\mathcal{L}_c(S)$ to get a finite subset of L_c.
2. (Local step) For each prime $p \in S$, computing $\mu_p(C(\mathbb{Q}_p))$.
3. Computing algebras $\mathcal{A}_\ell(P) := \text{ Cor }((\ell, \mu_p(P))_2)$ for required $\ell \in L^*$, prime $p \in S$, and $P \in C(\mathbb{Q}_p)$.

Reasons or the computation

Let $C : y^2 = f(x)$ be a hyperelliptic curve. Define $\Phi_\ell : C(\mathbb{A}_\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$ as

$$\Phi_\ell((x_p)_{p\leq\infty}) := \sum_{p\leq\infty} inv_p \mathcal{A}_\ell(x_p)$$

For $\bar{\ell} \in \mathcal{L}_c(S)$, we have $C(\mathbb{A}_\mathbb{Q})^{\gamma(\ell)} = \{x = (x_p) \in C(\mathbb{A}_\mathbb{Q}) : \Phi_\ell(x) = 0\}$

Theorem

Let $S = \{p_1, \ldots, p_n\}$ such that $\mu_p(C(\mathbb{Q}_p))$ is unramified at all $p \notin S$. If for each $W = (W_p)_{p\leq\infty} \in C(\mathbb{A}_\mathbb{Q})$, there is some ℓ_e such that $\Phi_{\ell_e}(W) = 1/2$, then $C(\mathbb{A}_\mathbb{Q})^{\gamma(L_c(S))} = \varnothing$. The converse also holds.

Result 2

Result 2

Let $\mathcal{L}_c(S) = \{\bar{\ell_1}, \bar{\ell_2}, \ldots, \bar{\ell_m}\}$, such that $\ell_1, \ldots, \ell_m \in L_c(S)$ is a set of distinct representatives of $\mathcal{L}_c(S)$.
Let $S = \{p_1, p_2, \ldots, p_n\}$
Let $I_S := \prod_{i=1}^{n} \mu_{p_i}(C(\mathbb{Q}_{p_i}))$. Define

$$\mu_S : C(\mathbb{A}_{\mathbb{Q}}) \longrightarrow I_S$$

$$P \longmapsto (\mu_{p_i}(P_{p_i}))_{i=1}^{n}.$$

Let $\mu_{p_i}(C(\mathbb{Q}_{p_i})) = \{a_1^{(i)}, a_2^{(i)}, \ldots, a_{j_i}^{(i)}\}$. Define the map

$$\Psi_\ell : I_S \longrightarrow \mathbb{Q}/\mathbb{Z}$$

$$(a_j^{(i)})_{i=1}^{n} \longmapsto \sum_{i=1}^{n} inv_{p_i}\ Cor((\ell, a_j^{(i)})_2).$$

In actual computation, however, we would not need to address adelic points directly. Instead, it is enough to deal with the image of the μ_p map for all primes $p \in S$.

Corollary

Let $S = \{p_1, \ldots, p_n\}$ be a finite set of primes such that the image $\mu_p(C(\mathbb{Q}_p))$ is unramified at all primes $p \notin S$. If for each element $(a_j^{(i)}) \in I_S$, there is some ℓ_e such that $\Psi_{\ell_e}((a_j^{(i)})_{i,j}) = 1/2$, then $C(\mathbb{A}_{\mathbb{Q}})^{\gamma(L_c(S))} = \varnothing$, i.e. $\gamma(L_c(S))$ obstructs the existence of rational points on the curve C. The converse also holds.

Advantages over Descent and M-W Sieve

1. Descent based computational methods are heavy, require class group and unit group calculations: practical when assuming Generalised Riemann Hypothesis (GRH) holds.
2. Mordell-Weil sieve based methods require $k-$rational points on Jacobians. This requires descent to get an upper bound for the rank.
3. Given a curve C, it is known that the subset $C(\mathbb{A})^{\mathrm{Br}\ C[2]}$ is the same as that cut out by $C(\mathbb{A})^{\text{2-ab}}$ (as shown in [Sto07],[CV15]). Scharaschkin [Sch99] proved that under certain conditions on the Tate-Shafarevich group, the potential obstruction to k-rational points coming from Mordell-Weil sieve method is a part of the Brauer-Manin obstruction.

The Brauer-Manin obstruction method:

1. relates to descent and Mordell-Weil sieve method: the results might provide alternate methods to find objects described through descent methods.
2. could help make computations unconditional, (by delivering a 'certificate' which does not depend on GRH), possibly less computationally intensive.
3. The results coming from this method would be readily checkable: our algorithm would aim to produce the minimal possible (finite) subset of the Brauer group that causes the obstruction. Other researchers can confirm our results independently at a very small computational cost.