

Computing Selmer groups of Jacobians

Edward Schaefer
Department of Mathematics
and Computer Science
Santa Clara University

Let C be a curve over K , a number field. We want to determine $C(K)$, the K -rational points on C .

General program (Bruin, Flynn, Poonen, Schaefer, Stoll, Wetherell, etc.):

Let J be the Jacobian of C . $J = \text{Div}^0(C)/\text{Princ}(C)$.

Elliptic curves are Jacobians: $E \cong \text{Div}^0(E)/\text{Princ}(E)$ by $P \mapsto [P - 0]$.

We know $J(K) \cong \mathbf{Z}^r \oplus J(K)_{\text{tors}}$ where r and $\#J(K)_{\text{tors}}$ are finite.

Find $C(K)$. $J = \text{Div}^0(C)/\text{Princ}(C)$.

$$J(K) \cong \mathbf{Z}^r \oplus J(K)_{\text{tors}}.$$

1. Determine $J(K)_{\text{tors}}$. \exists effective algorithm.
2. Find a Selmer group to give an upper bound for r .
(Focus of this talk.)
3. Find independent points of infinite order in $J(K)$ to give a lower bound for r .

If those bounds are the same, then you have r and a set of points in $J(K)$ generating a subgroup of finite index. Let's assume this.

If $r < \text{genus}(C)$ then continue. If not, use covering covers.

4. Use a Chabauty argument on C or its covers, (involving the pseudo-generating points) to determine $C(K)$ (not guaranteed to work).

How to use a Selmer group to find an upper bound for r when $J(K) \cong \mathbf{Z}^r \oplus J(K)_{\text{tors}}$.

Let p be prime. Assume we know $J(K)_{\text{tors}}$. If we knew $J(K)/pJ(K)$ then we'd know r .

There is no known effective algorithm for determining $J(K)/pJ(K)$.

There is an effectively computable (in theory) group called the Selmer group containing this group.

We have an exact sequence

$$0 \rightarrow J(\overline{K})[p] \rightarrow J(\overline{K}) \xrightarrow{p} J(\overline{K}) \rightarrow 0$$

of $\text{Gal}(\overline{K}/K)$ -modules.

Taking $\text{Gal}(\overline{K}/K)$ -invariants gives us

$$\begin{aligned} \dots J(K) \xrightarrow{p} J(K) \xrightarrow{\delta} H^1(\text{Gal}(\overline{K}/K), J[p]) \\ \rightarrow H^1(\text{Gal}(\overline{K}/K), J(\overline{K})) \xrightarrow{p} H^1(\text{Gal}(\overline{K}/K), J(\overline{K})) \rightarrow \\ \dots \end{aligned}$$

Giving us a short exact sequence

$$0 \rightarrow J(K)/pJ(K) \xrightarrow{\delta} H^1(K, J[p]) \rightarrow H^1(K, J)[p] \rightarrow 0.$$

(Note abbreviation of $\text{Gal}(\overline{K}/K)$ in H^1 .)

$$0 \rightarrow J(K)/pJ(K) \xrightarrow{\delta} H^1(K, J[p]) \rightarrow H^1(K, J)[p] \rightarrow 0.$$

We'd like to find $J(K)/pJ(K)$.

Equivalently, find its image in $H^1(K, J[p])$. Let S be the set of primes of K containing primes over p , primes of bad reduction of C and if $p = 2$, infinite primes.

Image of $J(K)/pJ(K)$ is contained in $H^1(K, J[p]; S)$, a finite group.

Approximate image locally.

$$\begin{array}{ccc} J(K)/pJ(K) & \xrightarrow{\delta} & H^1(K, J[p]; S) \\ \downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod \text{res}_{\mathfrak{s}} \\ \prod_{\mathfrak{s} \in S} J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}}) & \xrightarrow{\prod \delta_{\mathfrak{s}}} & \prod_{\mathfrak{s} \in S} H^1(K_{\mathfrak{s}}, J[p]) \end{array}$$

$$\begin{array}{ccc}
J(K)/pJ(K) & \xrightarrow{\delta} & H^1(K, J[p]; S) \\
\downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod \text{res}_{\mathfrak{s}} \\
\prod_{\mathfrak{s} \in S} J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}}) & \xrightarrow{\prod \delta_{\mathfrak{s}}} & \prod_{\mathfrak{s} \in S} H^1(K_{\mathfrak{s}}, J[p])
\end{array}$$

Want image of $J(K)/pJ(K)$ in $H^1(K, J[p]; S)$.

Define $S^p(K, J) = \{\gamma \in H^1(K, J[p]; S) \mid \text{res}_{\mathfrak{s}}(\gamma) \in \delta_{\mathfrak{s}}(J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}})) \quad \forall \mathfrak{s} \in S\}$.

Problems: 1) $H^1(K, J[p]; S)$ hard to work in.

2) $\delta_{\mathfrak{s}}$ hard to evaluate.

Solution: Replace group and map.

Replace $H^1(K, J[p])$.

Let \bar{A} be the étale K -algebra which is the set of maps from $J[p] \setminus 0$ to \bar{K} .

Let A be its $\text{Gal}(\bar{K}/K)$ -invariants.

What does it look like?

Let $J[p] \setminus 0 = \{T_1, \dots, T_l\}$.

(Note $l = p^{2g} - 1$.)

Concretely, $A = \prod^\diamond K(T_i)$ where \prod^\diamond means take one representative from each $\text{Gal}(\bar{K}/K)$ -orbit.

Replace $H^1(K, J[p])$.

Let \bar{A} be the étale K -algebra which is the maps from $J[p] \setminus 0$ to \bar{K} .

Let $\mu_p(\bar{A})$ be the maps from $J[p] \setminus 0$ to μ_p .

Let $w : J[p] \rightarrow \mu_p(\bar{A})$ by $P \mapsto (T_i \mapsto e_p(P, T_i))$.

This induces a map $\hat{w} : H^1(K, J[p]) \rightarrow H^1(K, \mu_p(\bar{A}))$.

Kummer theory induces an isomorphism
 $k : H^1(K, \mu_p(\bar{A})) \rightarrow A^\times / (A^\times)^p$.

Have $H^1(K, J[p]) \xrightarrow{\hat{w}} H^1(K, \mu_p(\overline{A})) \xrightarrow{k} A^\times / (A^\times)^p$.

Concerns: 1) Sure helps if \hat{w} is injective (doesn't have to be, though w is).

2) Need to find image of $H^1(K, J[p])$ in $A^\times / (A^\times)^p$ (can be difficult if smallest Galois-invariant spanning set of $J[p]$ is much larger than a basis).

3) Really need image of $H^1(K, J[p]; S)$ in $A(S, p) \subset A^\times / (A^\times)^p$. Requires class group/unit group information in number fields making up A .

Let's assume w is injective and we've found the image of $H^1(K, J[p]; S)$ in $A(S, p)$.

Have isomorphic image of $H^1(K, J[p]; S)$ in $A(S, p) \subset A^\times / (A^\times)^p$. Need to replace map

$$J(K)/pJ(K) \xrightarrow{\delta} H^1(K, J[p]) \xrightarrow{\hat{w}} H^1(K, \mu_p(\overline{A})) \xrightarrow{k} A(S, p).$$

Assume $C(K)$ non-empty. Then can choose divisors D_1, \dots, D_l , with $[D_i] = T_i \in J[p] \setminus 0$ and $pD_i = \text{div}_{f_i}$ and where $\{f_i\} \cong J[p] \setminus 0$ as $\text{Gal}(\overline{K}/K)$ -sets.

We call D a good divisor if $D \in \text{Div}^0(C)(K)$ and its support does not intersect any of the div_{f_i} 's.

Define $f : \{ \text{good divisors} \} \rightarrow A^*$
by $(D) \mapsto (T_i \mapsto f_i(D))$.

Theorem: The map f induces a well defined homomorphism from $J(K)/pJ(K) \rightarrow A(S, p) \subset A^\times / (A^\times)^p$ that is the same as $k\hat{w}\delta$.

Theorem: The map f induces a well defined homomorphism from $J(K)/pJ(K) \rightarrow A(S, p) \subset A^\times/(A^\times)^p$ that is the same as $k\hat{w}\delta$.

Equivalently we have

$$J(K)/pJ(K) \xrightarrow{\prod^\diamond f_i} \prod^\diamond K(T_i)(S, p) \subset K(T_i)^\times/(K(T_i)^\times)^p.$$

We have $A(S, p) = \prod^\diamond K(T_i)(S, p)$.

$$\begin{array}{ccc} J(K)/pJ(K) & \xrightarrow{f} & A(S, p) \\ \downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod \beta_{\mathfrak{s}} \\ \prod_{\mathfrak{s} \in S} J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}}) & \xrightarrow{f} & \prod_{\mathfrak{s} \in S} A_{\mathfrak{s}}^\times/(A_{\mathfrak{s}}^\times)^p \end{array}$$

$$\begin{array}{ccc}
J(K)/pJ(K) & \xrightarrow{f} & A(S, p) \\
\downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod \beta_{\mathfrak{s}} \\
\prod_{\mathfrak{s} \in S} J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}}) & \xrightarrow{f} & \prod_{\mathfrak{s} \in S} A_{\mathfrak{s}}^{\times}/(A_{\mathfrak{s}}^{\times})^p
\end{array}$$

or (noting $K(T_i)(S, p) \subset K(T_i)^{\times}/(K(T_i)^{\times})^p$)

$$\begin{array}{ccc}
J(K)/pJ(K) & \xrightarrow{\prod^{\diamond} f_i} & \prod^{\diamond} K(T_i)(S, p) \\
\downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod^{\diamond} \beta_{\mathfrak{s}, i} \\
\prod_{\mathfrak{s} \in S} J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}}) & \xrightarrow{\prod^{\diamond} f_i} & \prod_{\mathfrak{s} \in S}^{\diamond} K(T_i)_{\mathfrak{s}}^{\times}/(K(T_i)_{\mathfrak{s}}^{\times})^p
\end{array}$$

We have $S^p(K, J) = \{\gamma \in \text{image of } H^1(K, J[p]) \text{ in } A(S, p) \mid \beta_{\mathfrak{s}}(\gamma) \in f(J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}})) \ \forall \mathfrak{s} \in S\}$.

Notes:

1. If have isogeny $\phi : B \rightarrow J$ over K where B is an abelian variety then can use this technique to find $S^\phi(K, B)$.

2. Instead of using all of $J[p] \setminus 0$ can use a Galois-invariant spanning set of $J[p]$. Will get lower degree A .

Important related method.

Above, had $\text{div}(f_i) = pD_i$. What if

What if $\text{div}(f_i) = pD_i - D'$ where D_i effective and D'/K ?

Example: Hyperelliptic curve. Generically, a hyperelliptic curve of genus g has equation $y^2 = h(x)$, where $h(x)$ has degree $2g + 2$.

Let $h(\alpha_i) = 0$ and consider $f_i = x - \alpha_i$ then $\text{div}(f_i) = 2(\alpha_i, 0) - (\infty^+ + \infty^-)$.

Example: Hyperelliptic curve. Generically, a hyperelliptic curve of genus g has equation $y^2 = h(x)$, where $h(x)$ has degree $2g + 2$.

For $1 \leq i \leq 2g+2$, let $h(\alpha_i) = 0$ and consider $f_i = x - \alpha_i$ then $\text{div}(f_i) = 2(\alpha_i, 0) - (\infty^+ + \infty^-)$.

Note their differences are $\{2(\alpha_i, 0) - 2(\alpha_j, 0)\}$ and the set $\{[(\alpha_i, 0) - (\alpha_j, 0)]\}$ spans $J[2]$.

Let \overline{A} be the set of maps from $\{2(\alpha_i, 0) - (\infty^+ - \infty^-)\}$ to \overline{K} .

So $A \cong K[T]/(h(T))$ and $f = x - T$.

$$J(K)/2J(K) \xrightarrow{x-T} A^\times / (A^{\times 2} K^\times).$$

Has kernel of size 1 or 2, depending on Galois-action on roots of h .

Let $C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$.

Has known rational points $(0, \pm 1)$, $(-3, \pm 1)$, ∞^+ , ∞^- .

$\#J(\mathbf{F}_3) = 9$ and $\#J(\mathbf{F}_5) = 41$ so $J(\mathbf{Q})_{\text{tors}} = 0$. Thus $J(\mathbf{Q}) \cong \mathbf{Z}^r$.

We have

$A = \mathbf{Q}[T]/(T^6 + 8T^5 + 22T^4 + 22T^3 + 5T^2 + 6T + 1)$,
a sextic number field.

From Galois-action on roots of sextic, we find index of $2J(\mathbf{Q})$ in $\ker(x - T)$ is 2.

Let $C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$.

We have

$A = \mathbf{Q}[T]/(T^6 + 8T^5 + 22T^4 + 22T^3 + 5T^2 + 6T + 1)$,
a sextic number field.

Bad primes are $S = \{\infty, 2, 3701\}$.

$$\begin{array}{ccc} J(\mathbf{Q})/2J(\mathbf{Q}) & \xrightarrow{x-T} & A^\times/(A^{\times 2}\mathbf{Q}^\times) \\ \downarrow & & \downarrow \prod \beta_p \\ \prod_{p \in S} J(\mathbf{Q}_p)/2J(\mathbf{Q}_p) & \xrightarrow{x-T} & \prod_{p \in S} A_p^\times/(A_p^{\times 2}\mathbf{Q}_p^\times) \end{array}$$

Define $S_{\text{fake}}^2(\mathbf{Q}, J) = \{\gamma \in \ker N : A(S, 2)/\mathbf{Q}(S, 2) \rightarrow \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \mid \beta_p(\gamma) \in (x - T)(J(\mathbf{Q}_p)) \forall p \in S\}$.

From Galois action on zeros of sextic, turns out
 $\dim_{\mathbf{F}_2} S^2(\mathbf{Q}, J) = \dim_{\mathbf{F}_2} S_{\text{fake}}^2(\mathbf{Q}, J) + 1$.

We have $A = \mathbf{Q}[T]/(T^6 + 8T^5 + 22T^4 + 22T^3 + 5T^2 + 6T + 1)$ - a sextic number field.

$$\begin{array}{ccc} J(\mathbf{Q})/2J(\mathbf{Q}) & \xrightarrow{x-T} & A^\times/(A^{\times 2}\mathbf{Q}^\times) \\ \downarrow & & \downarrow \prod \beta_p \\ \prod_{p \in S} J(\mathbf{Q}_p)/2J(\mathbf{Q}_p) & \xrightarrow{x-T} & \prod_{p \in S} A_p^\times/(A_p^{\times 2}\mathbf{Q}_p^\times) \end{array}$$

Basis of $A(S, 2)$ is $\{-1, u_1, u_2, u_3, \alpha, \beta_1, \beta_2, \beta_3\}$ with norms $\{1, 1, 1, -1, 2^3, 3701, -3701, 3701^3\}$.

Basis of $\ker N : A(S, 2)/\mathbf{Q}(S, 2) \rightarrow \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ is $\{u_1, u_3\beta_1\beta_2\}$.
So $S_{\text{fake}}^2(\mathbf{Q}, J) \subseteq \langle u_1, u_3\beta_1\beta_2 \rangle$.

The image of $J(\mathbf{Q}_{3701})$ in $A_{3701}^\times/(A_{3701}^{\times 2}\mathbf{Q}_{3701}^\times)$ is generated by the image of $[(-4, \sqrt{185}) - \infty^-]$. It is a unit in each component. So $u_3\beta_1\beta_2$ and $u_1u_3\beta_1\beta_2$ do not map to $(x - T)J(\mathbf{Q}_{3701})$. Thus $S_{\text{fake}}^2(\mathbf{Q}, J) \subseteq \langle u_1 \rangle$.

The image of $J(\mathbf{Q}_2)$ in $A_2^\times/(A_2^{\times 2}\mathbf{Q}_2^\times)$ is the image of $\langle [(2, \sqrt{881}) - \infty^-] \rangle$ and u_1 does not map to that.
So $S_{\text{fake}}^2(\mathbf{Q}, J)$ is trivial.

We have $S_{\text{fake}}^2(\mathbf{Q}, J)$ is trivial.

Since $\dim_{\mathbf{F}_2} S^2(\mathbf{Q}, J) = \dim_{\mathbf{F}_2} S_{\text{fake}}^2(\mathbf{Q}, J)$,
we have $\dim_{\mathbf{F}_2} S^2(\mathbf{Q}, J) = 1$.

Since $J(\mathbf{Q})/2J(\mathbf{Q}) \subseteq S^2(\mathbf{Q}, J)$,
we have $\dim_{\mathbf{F}_2} J(\mathbf{Q})/2J(\mathbf{Q}) \leq 1$.

It's easy to show that $[\infty^+ - \infty^-]$ has infinite order.

So $1 \leq \dim_{\mathbf{F}_2} J(\mathbf{Q})/2J(\mathbf{Q})$.

Thus $\dim_{\mathbf{F}_2} J(\mathbf{Q})/2J(\mathbf{Q}) = 1$.

Since $J(\mathbf{Q}) \cong \mathbf{Z}^r$ we have $J(\mathbf{Q}) \cong \mathbf{Z}$.

Chabauty argument shows for

$$C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1,$$

we have $C(\mathbf{Q}) = \{(0, \pm 1), (-3, \pm 1), \infty^\pm\}$.

References:

General case:

Schaefer, E.F. *Computing a Selmer group of a Jacobian using functions on the curve*, *Mathematische Annalen*, **310**, 1998, 447–471.

$y^2 = f(x)$ case:

Flynn, E.V., Poonen, B. and Schaefer, E.F. *Cycles of quadratic polynomials and rational points on a genus-2 curve*, *Duke Mathematical Journal*, **90**, 1997, 435–463.

$y^p = f(x)$ case:

Poonen, B. and Schaefer, E.F. *Explicit Descent for Jacobians of cyclic covers of the projective line*, *Journal für die reine und angewandte Mathematik*, **488**, 1997, 141–188.