Descent and Covering Collections
Part III: The Fake 2-Selmer Set

Michael Stoll
Universität Bayreuth

NATO Advanced Study Institute
Ohrid

September 5, 2014

Double Covers

Proposition.
Let $C\colon y^2 = F_1(x,z)F_2(x,z)$ with $\deg F_1$, $\deg F_2$ even, and set

$$\mathcal{S} = \left\{ d \in \mathbb{Z} : d \text{ squarefree and } \forall p\colon p \mid d \Rightarrow p \mid \operatorname{Res}(F_1, F_2) \right\}.$$

The $\mathcal{S}$ is finite and

$$C(\mathbb{Q}) = \bigcup_{d \in \mathcal{S}} \pi_d\big(D_d(\mathbb{Q})\big)\,,$$

where $\quad D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$
and $\quad \pi_d\colon D_d \to C,\ (x : y_1 : y_2 : z) \mapsto (x : dy_1y_2 : z)$.

We write $D = D_1$ and $\pi = \pi_1\colon D \to C$. Then

$$\operatorname{Sel}(\pi) = \{ d \in \mathcal{S} : D_d \text{ is ELS} \}.$$

No Double Cover

What can we do if $C\colon y^2 = f(x)$ does not admit an unramified double cover?

No Double Cover

What can we do if $C\colon y^2 = f(x)$ does not admit an unramified double cover?

The right hand side $f(x)$ may not factor over $\mathbb{Q}$,
but it does so over suitable field extensions.

No Double Cover

What can we do if $C\colon y^2 = f(x)$ does not admit an unramified double cover?

The right hand side $f(x)$ may not factor over $\mathbb{Q}$,
but it does so over suitable field extensions.
The corresponding double covers are permuted by the Galois group,
so by combining them, we obtain a covering defined over $\mathbb{Q}$ again.

No Double Cover

What can we do if $C\colon y^2 = f(x)$ does not admit an unramified double cover?

The right hand side $f(x)$ may not factor over $\mathbb{Q}$,
but it does so over suitable field extensions.
The corresponding double covers are permuted by the Galois group,
so by combining them, we obtain a covering defined over $\mathbb{Q}$ again.

What we obtain in this way is a 2-covering of C,
obtained by pulling back C via the multiplication-by-2 map on its Jacobian.

No Double Cover

What can we do if $C\colon y^2 = f(x)$ does not admit an unramified double cover?

The right hand side $f(x)$ may not factor over $\mathbb{Q}$,
but it does so over suitable field extensions.
The corresponding double covers are permuted by the Galois group,
so by combining them, we obtain a covering defined over $\mathbb{Q}$ again.

What we obtain in this way is a 2-covering of C,
obtained by pulling back C via the multiplication-by-2 map on its Jacobian.

The corresponding Selmer set is the 2-Selmer set, $\mathrm{Sel}_2(C)$.

A Way of Computing $\mathrm{Sel}_2(C)$

Assume we have fixed a rational divisor class of degree 1 on C and thus an embedding $\iota \colon C \to J$, where J is the Jacobian of C.

A Way of Computing $\mathrm{Sel}_2(C)$

Assume we have fixed a rational divisor class of degree 1 on C and thus an embedding $i\colon C \to J$, where J is the Jacobian of C.

Then we can identify $\mathrm{Sel}_2(C)$ with the subset of $\mathrm{Sel}_2(J)$ consisting of all classes ξ whose image in $J(\mathbb{Q}_v)/2J(\mathbb{Q}_v)$ is contained in the image of $i\bigl(C(\mathbb{Q}_v)\bigr)$, for all places v.
(This means $v = p$ a prime or $v = \infty$ with $\mathbb{Q}_\infty = \mathbb{R}$.)

A Way of Computing $\mathrm{Sel}_2(C)$

Assume we have fixed a rational divisor class of degree 1 on C and thus an embedding $i\colon C \to J$, where J is the Jacobian of C.

Then we can identify $\mathrm{Sel}_2(C)$ with the subset of $\mathrm{Sel}_2(J)$ consisting of all classes ξ whose image in $J(\mathbb{Q}_v)/2J(\mathbb{Q}_v)$ is contained in the image of $i\big(C(\mathbb{Q}_v)\big)$, for all places v.
(This means $v = p$ a prime or $v = \infty$ with $\mathbb{Q}_\infty = \mathbb{R}$.)

Interpretation:
The condition for ξ at v is equivalent to $D_\xi(\mathbb{Q}_v) \neq \emptyset$, but can be checked without constructing D_ξ.

The Étale Algebra

Fix a hyperelliptic curve

$$C\colon y^2 = f(x)\,.$$

We define (compare Steffen's lectures)

$$A = \mathbb{Q}[x]/\langle f(x)\rangle \qquad \text{and} \qquad A_v = A \otimes_{\mathbb{Q}} \mathbb{Q}_v = \mathbb{Q}_v[x]/\langle f(x)\rangle$$

for all places v.

The Étale Algebra

Fix a hyperelliptic curve

$$C\colon y^2 = f(x)\,.$$

We define (compare Steffen's lectures)

$$A = \mathbb{Q}[x]/\langle f(x)\rangle \qquad \text{and} \qquad A_v = A \otimes_{\mathbb{Q}} \mathbb{Q}_v = \mathbb{Q}_v[x]/\langle f(x)\rangle$$

for all places v. Then A is an étale $\mathbb{Q}$-algebra:
it splits as a product of finite field extensions of $\mathbb{Q}$.
Similarly, A_v is an étale $\mathbb{Q}_v$-algebra.

The Étale Algebra

Fix a hyperelliptic curve

$$C\colon y^2 = f(x)\,.$$

We define (compare Steffen's lectures)

$$A = \mathbb{Q}[x]/\langle f(x)\rangle \qquad \text{and} \qquad A_v = A \otimes_{\mathbb{Q}} \mathbb{Q}_v = \mathbb{Q}_v[x]/\langle f(x)\rangle$$

for all places v. Then A is an étale $\mathbb{Q}$-algebra:
it splits as a product of finite field extensions of $\mathbb{Q}$.
Similarly, A_v is an étale $\mathbb{Q}_v$-algebra.

We denote the image of x in A or A_v by T, so $A = \mathbb{Q}[T]$ and $A_v = \mathbb{Q}_v[T]$.
We can think of T as a 'generic root' of f.

The Étale Algebra

Fix a hyperelliptic curve

$$C\colon y^2 = f(x)\,.$$

We define (compare Steffen's lectures)

$$A = \mathbb{Q}[x]/\langle f(x)\rangle \qquad \text{and} \qquad A_v = A \otimes_{\mathbb{Q}} \mathbb{Q}_v = \mathbb{Q}_v[x]/\langle f(x)\rangle$$

for all places v. Then A is an étale $\mathbb{Q}$-algebra:
it splits as a product of finite field extensions of $\mathbb{Q}$.
Similarly, A_v is an étale $\mathbb{Q}_v$-algebra.

We denote the image of x in A or A_v by T, so $A = \mathbb{Q}[T]$ and $A_v = \mathbb{Q}_v[T]$.
We can think of T as a 'generic root' of f.

We write $A^{\square} = \{\alpha^2 : \alpha \in A^{\times}\}$; analogously for $\mathbb{Q}^{\square}$.

The $x - T$ Map

For the following, we assume that $f \in \mathbb{Z}[x]$
and that f is monic if $\deg f$ is odd (this can always be achieved).

The $x - T$ Map

For the following, we assume that $f \in \mathbb{Z}[x]$
and that f is monic if $\deg f$ is odd (this can always be achieved).

Set

$$H = \begin{cases} \{\alpha \in A^\times/A^\square : N_{A/\mathbb{Q}}(\alpha) = \mathbb{Q}^\square\} & \text{if } \deg f \text{ is odd;} \\ \{\alpha \in A^\times/(\mathbb{Q}^\times A^\square) : N_{A/\mathbb{Q}}(\alpha) = \mathrm{lcf}(f)\mathbb{Q}^\square\} & \text{if } \deg f \text{ is even.} \end{cases}$$

The $x - T$ Map

For the following, we assume that $f \in \mathbb{Z}[x]$
and that f is monic if $\deg f$ is odd (this can always be achieved).

Set

$$H = \begin{cases} \{\alpha \in A^\times/A^\square : N_{A/\mathbb{Q}}(\alpha) = \mathbb{Q}^\square\} & \text{if } \deg f \text{ is odd;} \\ \{\alpha \in A^\times/(\mathbb{Q}^\times A^\square) : N_{A/\mathbb{Q}}(\alpha) = \mathrm{lcf}(f)\mathbb{Q}^\square\} & \text{if } \deg f \text{ is even.} \end{cases}$$

Define H_v analogously in terms of A_v and $\mathbb{Q}_v$.

The $x - T$ Map

For the following, we assume that $f \in \mathbb{Z}[x]$
and that f is monic if $\deg f$ is odd (this can always be achieved).

Set

$$H = \begin{cases} \{\alpha \in A^\times/A^\square : N_{A/\mathbb{Q}}(\alpha) = \mathbb{Q}^\square\} & \text{if } \deg f \text{ is odd;} \\ \{\alpha \in A^\times/(\mathbb{Q}^\times A^\square) : N_{A/\mathbb{Q}}(\alpha) = \operatorname{lcf}(f)\mathbb{Q}^\square\} & \text{if } \deg f \text{ is even.} \end{cases}$$

Define H_v analogously in terms of A_v and $\mathbb{Q}_v$.

There is a map $\delta \colon C(\mathbb{Q}) \longrightarrow H$, $P \longmapsto$ the class of $x(P) - T$,
(with some modification when $x(P) = \infty$ or when $y(P) = 0$);

The $x - T$ Map

For the following, we assume that $f \in \mathbb{Z}[x]$
and that f is monic if $\deg f$ is odd (this can always be achieved).

Set

$$H = \begin{cases} \{\alpha \in A^\times / A^\square : N_{A/\mathbb{Q}}(\alpha) = \mathbb{Q}^\square\} & \text{if } \deg f \text{ is odd;} \\ \{\alpha \in A^\times / (\mathbb{Q}^\times A^\square) : N_{A/\mathbb{Q}}(\alpha) = \mathrm{lcf}(f)\mathbb{Q}^\square\} & \text{if } \deg f \text{ is even.} \end{cases}$$

Define H_v analogously in terms of A_v and $\mathbb{Q}_v$.

There is a map $\delta\colon C(\mathbb{Q}) \longrightarrow H$, $P \longmapsto$ the class of $x(P) - T$,
(with some modification when $x(P) = \infty$ or when $y(P) = 0$);
analogously there is $\delta_v\colon C(\mathbb{Q}_v) \to H_v$ for each place v.

Compare the construction in Steffen's talk!

A Diagram

The maps fit together in a commutative diagram:

$$
\begin{array}{ccc}
C(\mathbb{Q}) & \xrightarrow{\quad\delta\quad} & H \\
\big\downarrow & & \big\downarrow {\scriptstyle (\rho_v)_v} \\
\prod_v C(\mathbb{Q}_v) & \xrightarrow{\prod \delta_v} & \prod_v H_v
\end{array}
$$

where $\rho_v \colon H \to H_v$ is the canonical map induced by $\mathbb{Q} \subset \mathbb{Q}_v$.

A Diagram

The maps fit together in a commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\quad \delta \quad} & H \\ \big\downarrow & & \big\downarrow {\scriptstyle (\rho_v)_v} \\ \prod_v C(\mathbb{Q}_v) & \xrightarrow{\ \prod \delta_v\ } & \prod_v H_v \end{array}$$

where $\rho_v \colon H \to H_v$ is the canonical map induced by $\mathbb{Q} \subset \mathbb{Q}_v$.

Definition.

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \{\alpha \in H : \forall v \colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\}$$

is the fake 2-Selmer set of C.

Relation With the 2-Selmer Set

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H : \forall v \colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

Relation With the 2-Selmer Set

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H : \forall v \colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

Clearly, δ maps $C(\mathbb{Q})$ into $\mathrm{Sel}_2^{\mathrm{fake}}(C)$, so $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$ implies $C(\mathbb{Q}) = \emptyset$.

Relation With the 2-Selmer Set

$$\mathrm{Sel}_2^{\text{fake}}(C) = \left\{\alpha \in H : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

Clearly, δ maps $C(\mathbb{Q})$ into $\mathrm{Sel}_2^{\text{fake}}(C)$, so $\mathrm{Sel}_2^{\text{fake}}(C) = \emptyset$ implies $C(\mathbb{Q}) = \emptyset$.

More precisely, the following holds.

Proposition.
There is a canonical surjective map $\mathrm{Sel}_2(C) \to \mathrm{Sel}_2^{\text{fake}}(C)$.
It is either a bijection or (usually) a two-to-one map.

Relation With the 2-Selmer Set

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \{\alpha \in H : \forall v \colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\} .$$

Clearly, δ maps $C(\mathbb{Q})$ into $\mathrm{Sel}_2^{\mathrm{fake}}(C)$, so $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$ implies $C(\mathbb{Q}) = \emptyset$.

More precisely, the following holds.

Proposition.
There is a canonical surjective map $\mathrm{Sel}_2(C) \to \mathrm{Sel}_2^{\mathrm{fake}}(C)$.
It is either a bijection or (usually) a two-to-one map.
(There is an explicit criterion for deciding which of the two is the case.)

Relation With the 2-Selmer Set

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \{\alpha \in H : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\}.$$

Clearly, δ maps $C(\mathbb{Q})$ into $\mathrm{Sel}_2^{\mathrm{fake}}(C)$, so $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$ implies $C(\mathbb{Q}) = \emptyset$.

More precisely, the following holds.

Proposition.
There is a canonical surjective map $\mathrm{Sel}_2(C) \to \mathrm{Sel}_2^{\mathrm{fake}}(C)$.
It is either a bijection or (usually) a two-to-one map.
(There is an explicit criterion for deciding which of the two is the case.)

In fact, $\mathrm{Sel}_2^{\mathrm{fake}}(C)$ classifies ELS 2-coverings $D \to C$ up to isomorphism and post-composition with the hyperelliptic involution of C.

Computing the Fake 2-Selmer Set (1)

Let Σ be $\{\infty, 2\}$, together with all prime divisors of $\mathrm{disc}(f)$ and of $\mathrm{lcf}(f)$.

Computing the Fake 2-Selmer Set (1)

Let Σ be $\{\infty, 2\}$, together with all prime divisors of $\mathrm{disc}(f)$ and of $\mathrm{lcf}(f)$.

This is a finite set of places, so the subgroup $A(\Sigma, 2) \subset A^\times / A^\square$ of elements 'unramified outside Σ' is finite and computable,

Computing the Fake 2-Selmer Set (1)

Let Σ be $\{\infty, 2\}$, together with all prime divisors of $\mathrm{disc}(f)$ and of $\mathrm{lcf}(f)$.

This is a finite set of places, so the subgroup $A(\Sigma, 2) \subset A^\times/A^\square$ of elements 'unramified outside Σ' is finite and computable, giving rise to a finite subset H_Σ of H.

Computing the Fake 2-Selmer Set (1)

Let Σ be $\{\infty, 2\}$, together with all prime divisors of $\mathrm{disc}(f)$ and of $\mathrm{lcf}(f)$.

This is a finite set of places, so the subgroup $A(\Sigma, 2) \subset A^\times/A^\square$ of elements 'unramified outside Σ' is finite and computable, giving rise to a finite subset H_Σ of H.

In a very similar way as for the Jacobian, one shows that $\mathrm{Sel}_2^{\mathrm{fake}}(C) \subset H_\Sigma$.

Computing the Fake 2-Selmer Set (1)

Let Σ be $\{\infty, 2\}$, together with all prime divisors of $\mathrm{disc}(f)$ and of $\mathrm{lcf}(f)$.

This is a finite set of places, so the subgroup $A(\Sigma, 2) \subset A^\times/A^\square$ of elements 'unramified outside Σ' is finite and computable, giving rise to a finite subset H_Σ of H.

In a very similar way as for the Jacobian, one shows that $\mathrm{Sel}_2^{\mathrm{fake}}(C) \subset H_\Sigma$.

This leads to

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

Computing the Fake 2-Selmer Set (1)

Let Σ be $\{\infty, 2\}$, together with all prime divisors of $\text{disc}(f)$ and of $\text{lcf}(f)$.

This is a finite set of places, so the subgroup $A(\Sigma, 2) \subset A^\times/A^\square$ of elements 'unramified outside Σ' is finite and computable, giving rise to a finite subset H_Σ of H.

In a very similar way as for the Jacobian, one shows that $\text{Sel}_2^{\text{fake}}(C) \subset H_\Sigma$.

This leads to

$$\text{Sel}_2^{\text{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v \colon \rho_v(\alpha) \in \text{im}(\delta_v)\right\}.$$

There are still infinitely many conditions to check, though!

Computing the Fake 2-Selmer Set (2)

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{ \alpha \in H_\Sigma : \forall v \colon \rho_v(\alpha) \in \mathrm{im}(\delta_v) \right\}.$$

Computing the Fake 2-Selmer Set (2)

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

For $p \notin \Sigma$, let H_p^0 be the 'unramified part' of H_p
(this is the part that comes from $\mathbb{Z}_p[T]$).

Computing the Fake 2-Selmer Set (2)

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

For $p \notin \Sigma$, let H_p^0 be the 'unramified part' of H_p
(this is the part that comes from $\mathbb{Z}_p[T]$).
We have

$$H_\Sigma = \left\{\alpha \in H : \forall p \notin \Sigma\colon \rho_p(\alpha) \in H_p^0\right\}.$$

Computing the Fake 2-Selmer Set (2)

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

For $p \notin \Sigma$, let H_p^0 be the 'unramified part' of H_p
(this is the part that comes from $\mathbb{Z}_p[T]$).
We have

$$H_\Sigma = \left\{\alpha \in H : \forall p \notin \Sigma\colon \rho_p(\alpha) \in H_p^0\right\}.$$

This means that we need to consider only the $p \notin \Sigma$ with $\mathrm{im}(\delta_p) \neq H_p^0$
(plus all $v \in \Sigma$, of course).

Computing the Fake 2-Selmer Set (2)

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \left\{\alpha \in H_\Sigma : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\right\}.$$

For $p \notin \Sigma$, let H_p^0 be the 'unramified part' of H_p
(this is the part that comes from $\mathbb{Z}_p[T]$).
We have

$$H_\Sigma = \left\{\alpha \in H : \forall p \notin \Sigma\colon \rho_p(\alpha) \in H_p^0\right\}.$$

This means that we need to consider only the $p \notin \Sigma$ with $\mathrm{im}(\delta_p) \neq H_p^0$
(plus all $v \in \Sigma$, of course).

Since $\rho_p(\alpha) \in \mathrm{im}(\delta_p)$ means $D_\alpha(\mathbb{Q}_p) \neq \emptyset$, by the Weil bounds,
we will always have $\mathrm{im}(\delta_p) = H_p^0$ for $p \notin \Sigma$ if $p \geq 4\,\mathrm{genus}(D)^2$.

Computing the Fake 2-Selmer Set (2)

$$\mathrm{Sel}_2^{\mathrm{fake}}(C) = \{\alpha \in H_\Sigma : \forall v\colon \rho_v(\alpha) \in \mathrm{im}(\delta_v)\}.$$

For $p \notin \Sigma$, let H_p^0 be the 'unramified part' of H_p
(this is the part that comes from $\mathbb{Z}_p[T]$).
We have

$$H_\Sigma = \{\alpha \in H : \forall p \notin \Sigma\colon \rho_p(\alpha) \in H_p^0\}.$$

This means that we need to consider only the $p \notin \Sigma$ with $\mathrm{im}(\delta_p) \neq H_p^0$
(plus all $v \in \Sigma$, of course).

Since $\rho_p(\alpha) \in \mathrm{im}(\delta_p)$ means $D_\alpha(\mathbb{Q}_p) \neq \emptyset$, by the Weil bounds,
we will always have $\mathrm{im}(\delta_p) = H_p^0$ for $p \notin \Sigma$ if $p \geq 4\,\mathrm{genus}(D)^2$.

Note that $\mathrm{genus}(D) = 4^g(g-1)+1$, so this bound is usually too large.

Computing the Fake 2-Selmer Set (3)

Still, these considerations show that we can compute $\mathrm{Sel}_2^{\mathrm{fake}}(C)$, if we can compute the 'local images' $\mathrm{im}(\delta_v)$.

Computing the Fake 2-Selmer Set (3)

Still, these considerations show that we can compute $\mathrm{Sel}_2^{\mathrm{fake}}(C)$, if we can compute the 'local images' $\mathrm{im}(\delta_v)$.

That this is possible follows from the fact that δ_v is locally constant:

Computing the Fake 2-Selmer Set (3)

Still, these considerations show that we can compute $\mathrm{Sel}_2^{\mathsf{fake}}(C)$,
if we can compute the 'local images' $\mathrm{im}(\delta_v)$.

That this is possible follows from the fact that δ_v is locally constant:
It is a continuous map from the compact space $C(\mathbb{Q}_v)$
to the discrete space H_v,

Computing the Fake 2-Selmer Set (3)

Still, these considerations show that we can compute $\mathrm{Sel}_2^{\mathsf{fake}}(C)$,
if we can compute the 'local images' $\mathrm{im}(\delta_v)$.

That this is possible follows from the fact that δ_v is locally constant:
It is a continuous map from the compact space $C(\mathbb{Q}_v)$
to the discrete space H_v,
so $C(\mathbb{Q}_v)$ splits into finitely many closed and open subsets
on which δ_v is constant.

Computing the Fake 2-Selmer Set (3)

Still, these considerations show that we can compute $\mathrm{Sel}_2^{\mathsf{fake}}(C)$, if we can compute the 'local images' $\mathrm{im}(\delta_v)$.

That this is possible follows from the fact that δ_v is locally constant:
It is a continuous map from the compact space $C(\mathbb{Q}_v)$
to the discrete space H_v,
so $C(\mathbb{Q}_v)$ splits into finitely many closed and open subsets
on which δ_v is constant.

These subsets can be explicitly described.

Computing the Fake 2-Selmer Set (3)

Still, these considerations show that we can compute $\mathrm{Sel}_2^{\mathrm{fake}}(C)$,
if we can compute the 'local images' $\mathrm{im}(\delta_v)$.

That this is possible follows from the fact that δ_v is locally constant:
It is a continuous map from the compact space $C(\mathbb{Q}_v)$
to the discrete space H_v,
so $C(\mathbb{Q}_v)$ splits into finitely many closed and open subsets
on which δ_v is constant.

These subsets can be explicitly described.

This gives an algorithm for computing $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

Computing the Fake 2-Selmer Set: Practice

In practice, we use a subset of the primes we would have to consider.
This results in a set S that contains $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

Computing the Fake 2-Selmer Set: Practice

In practice, we use a subset of the primes we would have to consider.
This results in a set S that contains $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

- If $S = \emptyset$, then $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$.

Computing the Fake 2-Selmer Set: Practice

In practice, we use a subset of the primes we would have to consider. This results in a set S that contains $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

- If $S = \emptyset$, then $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$.
- If we know $X \subset C(\mathbb{Q})$ such that $\delta(X) = S$, then $S = \mathrm{Sel}_2^{\mathrm{fake}}(C)$.

Computing the Fake 2-Selmer Set: Practice

In practice, we use a subset of the primes we would have to consider. This results in a set S that contains $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

- If $S = \emptyset$, then $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$.
- If we know $X \subset C(\mathbb{Q})$ such that $\delta(X) = S$, then $S = \mathrm{Sel}_2^{\mathrm{fake}}(C)$.

In many applications, one of these cases occurs.

Computing the Fake 2-Selmer Set: Practice

In practice, we use a subset of the primes we would have to consider.
This results in a set S that contains $\mathrm{Sel}_2^{\mathrm{fake}}(C)$.

- If $S = \emptyset$, then $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$.
- If we know $X \subset C(\mathbb{Q})$ such that $\delta(X) = S$, then $S = \mathrm{Sel}_2^{\mathrm{fake}}(C)$.

In many applications, one of these cases occurs.

The main computational bottleneck is the computation of $A(\Sigma, 2)$,
which involves computing ideal class groups and unit groups
of the number fields corresponding to the irreducible factors of f.

Examples

Together with **Nils Bruin**,
we considered all curves of genus 2 of height ≤ 3.

Examples

Together with **Nils Bruin**,
we considered all curves of genus 2 of height ≤ 3.

There are 196 171 isomorphism classes over $\mathbb{Q}$ of such curves.

Examples

Together with **Nils Bruin**,
we considered all curves of genus 2 of height ≤ 3.

There are 196 171 isomorphism classes over $\mathbb{Q}$ of such curves.

On 137 490 of these curves, one finds a (small) rational point.

Examples

Together with **Nils Bruin**,
we considered all curves of genus 2 of height ≤ 3.

There are 196 171 isomorphism classes over $\mathbb{Q}$ of such curves.

On 137 490 of these curves, one finds a (small) rational point.

Of the remaining 58 681 curves, 29 403 are not ELS.

Examples

Together with **Nils Bruin**,
we considered all curves of genus 2 of height ≤ 3.

There are 196 171 isomorphism classes over $\mathbb{Q}$ of such curves.

On 137 490 of these curves, one finds a (small) rational point.

Of the remaining 58 681 curves, 29 403 are not ELS.

Of the remaining 29 278 ELS curves C, 27 786 have $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$.

Examples

Together with **Nils Bruin**,
we considered all curves of genus 2 of height ≤ 3.

There are 196 171 isomorphism classes over $\mathbb{Q}$ of such curves.

On 137 490 of these curves, one finds a (small) rational point.

Of the remaining 58 681 curves, 29 403 are not ELS.

Of the remaining 29 278 ELS curves C, 27 786 have $\mathrm{Sel}_2^{\mathrm{fake}}(C) = \emptyset$.

For the last 1 492 curves C,
we could show that $C(\mathbb{Q}) = \emptyset$ using the Mordell-Weil sieve.

(For 42 curves, we had to assume BSD or GRH.)

A Recent Result

Recall the family $\mathcal{F}_g$ of all hyperelliptic curves of genus g, ordered by height.

A Recent Result

Recall the family $\mathcal{F}_g$ of all hyperelliptic curves of genus g, ordered by height.

Manjul **Bhargava** (one of this year's Fields medalists) was able to show that the average size of $\mathrm{Sel}_2^{\mathrm{fake}}(C)$ for $C \in \mathcal{F}_g$ tends to zero faster than 2^{-g} as $g \to \infty$.

A Recent Result

Recall the family $\mathcal{F}_g$ of all hyperelliptic curves of genus g, ordered by height.

Manjul **Bhargava** (one of this year's Fields medalists) was able to show that the average size of $\mathrm{Sel}_2^{\mathrm{fake}}(C)$ for $C \in \mathcal{F}_g$ tends to zero faster than 2^{-g} as $g \to \infty$.

This implies that the (upper) density of curves $C \in \mathcal{F}_g$ such that $\mathrm{Sel}_2^{\mathrm{fake}}(C) \neq \emptyset$ tends to zero faster than 2^{-g} as $g \to \infty$.

A Recent Result

Recall the family $\mathcal{F}_g$ of all hyperelliptic curves of genus g,
ordered by height.

Manjul **Bhargava** (one of this year's Fields medalists)
was able to show that the average size of $\mathrm{Sel}_2^{\mathrm{fake}}(C)$ for $C \in \mathcal{F}_g$
tends to zero faster than 2^{-g} as $g \to \infty$.

This implies that the (upper) density of curves $C \in \mathcal{F}_g$
such that $\mathrm{Sel}_2^{\mathrm{fake}}(C) \neq \emptyset$
tends to zero faster than 2^{-g} as $g \to \infty$.

This is based on results of Manjul's with Dick Gross
on the average behavior of 2-Selmer groups of hyperelliptic Jacobians.

Thank You!

These slides are available at

http://www.mathe2.uni-bayreuth.de/stoll/schrift.html#TalkNotes