Computing the H^1 of a π_1-module trivialised by a hyperelliptic covering

AGC^2 *T* 2023

Christophe Levrat

The question

Let $Y \to X$ be an unramified Galois covering of smooth curves over $\overline{\mathbb{F}_p}$ defined over $\mathbb{F}_p$. Let M be a f.g. $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module, where $p \neq \ell$.

The question

Let $Y \to X$ be an unramified Galois covering of smooth curves over $\overline{\mathbb{F}_p}$ defined over $\mathbb{F}_p$. Let M be a f.g. $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module, where $p \neq \ell$.

Question: How to compute $\mathrm{H}^1(\pi_1(X), M)$ with its Frobenius action?

The question

Let $Y \to X$ be an unramified Galois covering of smooth curves over $\overline{\mathbb{F}_p}$ defined over $\mathbb{F}_p$. Let M be a f.g. $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module, where $p \neq \ell$.

Question: How to compute $\mathrm{H}^1(\pi_1(X), M)$ with its Frobenius action?

Today: case where Y is hyperelliptic

Why??

- Why the question?

Why??

- Why the question?
  Ultimate goal: cohomology of surfaces

Why??

- Why the question?
  Ultimate goal: cohomology of surfaces
- What does it have to do with this talk?

Why??

- Why the question?
  Ultimate goal: cohomology of surfaces
- What does it have to do with this talk?
  Computation of the cohomology of constructible sheaves on curves

Why??

- Why the question?
  Ultimate goal: cohomology of surfaces
- What does it have to do with this talk?
  Computation of the cohomology of constructible sheaves on curves
  (talk at COGNAC $\rightarrow$ complexity not suitable for point counting)

Why??

- Why the question?
  Ultimate goal: cohomology of surfaces
- What does it have to do with this talk?
  Computation of the cohomology of constructible sheaves on curves
  (talk at COGNAC $\rightarrow$ complexity not suitable for point counting)
- Why a *hyperelliptic* covering?
  Because it's much easier than the general case! (but very specific)

π_1-modules

The general method

Applying it to hyperelliptic curves

Practical solutions (even for affine curves)

Cohomology of π_1-modules on curves

Let M be a finite ℓ-torsion $\pi_1(X)$-module, defined by an $\mathbb{F}_\ell$-representation of some $\mathrm{Aut}(Y|X)$, with $Y \to X$ étale Galois.

Cohomology of π_1-modules on curves

Let M be a finite ℓ-torsion $\pi_1(X)$-module, defined by an $\mathbb{F}_\ell$-representation of some $\mathrm{Aut}(Y|X)$, with $Y \to X$ étale Galois.

- If X is affine: $\mathrm{H}^i(\pi_1(X), M) = 0$ for all $i > 1$
- If X is projective: $\mathrm{H}^i(\pi_1(X), M) = 0$ for all $i > 2$ (and H^2 may be computed from H^0)

Cohomology of π_1-modules on curves

Let M be a finite ℓ-torsion $\pi_1(X)$-module, defined by an $\mathbb{F}_\ell$-representation of some $\mathrm{Aut}(Y|X)$, with $Y \to X$ étale Galois.

- If X is affine: $\mathrm{H}^i(\pi_1(X), M) = 0$ for all $i > 1$
- If X is projective: $\mathrm{H}^i(\pi_1(X), M) = 0$ for all $i > 2$ (and H^2 may be computed from H^0)
- From now on: write $\mathrm{H}^1(X, M)$ for $\mathrm{H}^1(\pi_1(X), M)$.

$$\mathrm{H}^1(X, M) = \frac{\{\phi\colon \pi_1(X) \to M \mid \phi(gh) = \phi(g) + g \cdot \phi(h)\}}{\{\phi\colon g \mapsto g \cdot m - m\}_{m \in M}}$$

An example: $\mathrm{H}^1(X, \mu_\ell)$

Let X be a smooth genus g curve over an algebraically closed field k. Denote by $\bar{X}$ its smooth compactification and set $r = |\bar{X} - X|$.

An example: $\mathrm{H}^1(X, \mu_\ell)$

Let X be a smooth genus g curve over an algebraically closed field k. Denote by $\bar{X}$ its smooth compactification and set $r = |\bar{X} - X|$.

$$\mathrm{H}^1(X, \mu_\ell) = \frac{\{(D, f) \in \mathrm{Div}(X) \times k(X) \mid \mathrm{div}(f) = \ell D\}}{\{(D, f) \mid f \in k(X)^\ell\}}$$

(one could also consider only the functions and forget about the divisors)

An example: $\mathrm{H}^1(X, \mu_\ell)$

Let X be a smooth genus g curve over an algebraically closed field k. Denote by $\bar{X}$ its smooth compactification and set $r = |\bar{X} - X|$.

$$\mathrm{H}^1(X, \mu_\ell) = \frac{\{(D, f) \in \mathrm{Div}(X) \times k(X) \mid \mathrm{div}(f) = \ell D\}}{\{(D, f) \mid f \in k(X)^\ell\}}$$

(one could also consider only the functions and forget about the divisors)

- ◇ When X is projective: $\mathrm{H}^1(X, \mu_\ell)$ has dimension $2g$ and is isomorphic to the ℓ-torsion $J_X[\ell]$ of the Jacobian of X

An example: $\mathrm{H}^1(X, \mu_\ell)$

Let X be a smooth genus g curve over an algebraically closed field k. Denote by $\bar{X}$ its smooth compactification and set $r = |\bar{X} - X|$.

$$\mathrm{H}^1(X, \mu_\ell) = \frac{\{(D, f) \in \mathrm{Div}(X) \times k(X) \mid \mathrm{div}(f) = \ell D\}}{\{(D, f) \mid f \in k(X)^\ell\}}$$

(one could also consider only the functions and forget about the divisors)

- ◇ When X is projective: $\mathrm{H}^1(X, \mu_\ell)$ has dimension $2g$ and is isomorphic to the ℓ-torsion $J_X[\ell]$ of the Jacobian of X
- ◇ When X is affine with r points at ∞: $\mathrm{H}^1(X, \mu_\ell)$ has dimension $2g - 1 + r$ additional points come from dividing by ℓ in J_X the points $P - Q$ where $P, Q \in \bar{X} - X$

π_1-modules

The general method

Applying it to hyperelliptic curves

Practical solutions (even for affine curves)

Suitable coverings

Let $Y \to X$ be an étale Galois covering of curves over $\overline{\mathbb{F}_p}$, defined over $\mathbb{F}_p$.
Les M a f.g. $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module.

Suitable coverings

Let $Y \to X$ be an étale Galois covering of curves over $\overline{\mathbb{F}_p}$, defined over $\mathbb{F}_p$.
Les M a f.g. $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module.
Consider an extension $\mathbb{F}_Q$ of $\mathbb{F}_p$ such that the action of $\mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$ on $\mathrm{H}^1(X, M)$ factors through $\mathrm{Gal}(\mathbb{F}_Q|\mathbb{F}_p)$.

Suitable coverings

Let $Y \to X$ be an étale Galois covering of curves over $\overline{\mathbb{F}_p}$, defined over $\mathbb{F}_p$.
Les M a f.g. $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module.
Consider an extension $\mathbb{F}_Q$ of $\mathbb{F}_p$ such that the action of $\mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$ on $\mathrm{H}^1(X, M)$ factors through $\mathrm{Gal}(\mathbb{F}_Q|\mathbb{F}_p)$.

Lemma

If $W \to Y$ is an étale covering such that:

- $W \to X$ is still Galois
- the map $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q) \to \mathrm{H}^1(W, \mu_\ell)$ is trivial

then there is a canonical isomorphism $\mathrm{H}^1(\mathrm{Aut}(W|X), M) \to \mathrm{H}^1(X, M)$.

Suitable coverings

Let $Y \to X$ be an étale Galois covering of curves over $\overline{\mathbb{F}_p}$, defined over $\mathbb{F}_p$.
Les M a f.g. $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module.
Consider an extension $\mathbb{F}_Q$ of $\mathbb{F}_p$ such that the action of $\mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$ on $\mathrm{H}^1(X, M)$ factors through $\mathrm{Gal}(\mathbb{F}_Q|\mathbb{F}_p)$.

Lemma

If $W \to Y$ is an étale covering such that:

- $W \to X$ is still Galois
- the map $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q) \to \mathrm{H}^1(W, \mu_\ell)$ is trivial

then there is a canonical isomorphism $\mathrm{H}^1(\mathrm{Aut}(W|X), M) \to \mathrm{H}^1(X, M)$.

$\to$ How to compute $\mathbb{F}_Q$ and W given X, M and Y?

Constructing such a covering

Set $r = |\bar{X} - X|$, $g_X = genus(X)$ and $m = \dim_{\mathbb{F}_\ell}(M)$.

Constructing such a covering

Set $r = |\bar{X} - X|$, $g_X = genus(X)$ and $m = \dim_{\mathbb{F}_\ell}(M)$.
$\mathrm{H}^1(X, M)$ is an $\mathbb{F}_\ell$-vector space of dimension $\leqslant m(2g_X + r)$.
Set $D = |\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)| \leqslant \ell^{(m(2g_X+r))^2}$ and $Q = p^D$.

Constructing such a covering

Set $r = |\bar{X} - X|$, $g_X = genus(X)$ and $m = \dim_{\mathbb{F}_\ell}(M)$.
$\mathrm{H}^1(X, M)$ is an $\mathbb{F}_\ell$-vector space of dimension $\leqslant m(2g_X + r)$.
Set $D = |\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)| \leqslant \ell^{(m(2g_X+r))^2}$ and $Q = p^D$.
Let $(f_1, \ldots, f_s)$ be a basis of $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q)$.

Constructing such a covering

Set $r = |\bar{X} - X|$, $g_X = genus(X)$ and $m = \dim_{\mathbb{F}_\ell}(M)$.
$\mathrm{H}^1(X, M)$ is an $\mathbb{F}_\ell$-vector space of dimension $\leqslant m(2g_X + r)$.
Set $D = |\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)| \leqslant \ell^{(m(2g_X+r))^2}$ and $Q = p^D$.
Let $(f_1, \ldots, f_s)$ be a basis of $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q)$.

- The covering $Y_D^{\langle \ell \rangle} \to Y$ with function field

$$k(Y_D^{\langle \ell \rangle}) = k(Y)\left(\sqrt[\ell]{f_1}, \ldots, \sqrt[\ell]{f_s}\right)$$

is an étale Galois covering of Y with group $\mathrm{Hom}(\mathrm{H}^1(Y, \mu_\ell), \mu_\ell)$.

Constructing such a covering

Set $r = |\bar{X} - X|$, $g_X = genus(X)$ and $m = \dim_{\mathbb{F}_\ell}(M)$.
$\mathrm{H}^1(X, M)$ is an $\mathbb{F}_\ell$-vector space of dimension $\leqslant m(2g_X + r)$.
Set $D = |\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)| \leqslant \ell^{(m(2g_X+r))^2}$ and $Q = p^D$.
Let $(f_1, \ldots, f_s)$ be a basis of $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q)$.

- The covering $Y_D^{\langle \ell \rangle} \to Y$ with function field

$$k(Y_D^{\langle \ell \rangle}) = k(Y)\left(\sqrt[\ell]{f_1}, \ldots, \sqrt[\ell]{f_s}\right)$$

  is an étale Galois covering of Y with group $\mathrm{Hom}(\mathrm{H}^1(Y, \mu_\ell), \mu_\ell)$.

- The map $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q) \to \mathrm{H}^1(Y_D^{\langle \ell \rangle}, \mu_\ell)$ is trivial.

Constructing such a covering

Set $r = |\bar{X} - X|$, $g_X = genus(X)$ and $m = \dim_{\mathbb{F}_\ell}(M)$.
$\mathrm{H}^1(X, M)$ is an $\mathbb{F}_\ell$-vector space of dimension $\leqslant m(2g_X + r)$.
Set $D = |\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)| \leqslant \ell^{(m(2g_X+r))^2}$ and $Q = p^D$.
Let $(f_1, \ldots, f_s)$ be a basis of $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q)$.

- The covering $Y_D^{\langle \ell \rangle} \to Y$ with function field

$$k(Y_D^{\langle \ell \rangle}) = k(Y)\left(\sqrt[\ell]{f_1}, \ldots, \sqrt[\ell]{f_s}\right)$$

  is an étale Galois covering of Y with group $\mathrm{Hom}(\mathrm{H}^1(Y, \mu_\ell), \mu_\ell)$.
- The map $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q) \to \mathrm{H}^1(Y_D^{\langle \ell \rangle}, \mu_\ell)$ is trivial.
- The covering $Y_D^{\langle \ell \rangle} \to X$ is still Galois.

π_1-modules

The general method

Applying it to hyperelliptic curves

Practical solutions (even for affine curves)

Point counting & ℓ-torsion

p-adic point counting :

- ◇ Kedlaya (2001): given genus g hyperelliptic curve X over $\mathbb{F}_{p^n}$, computes zeta function $Z_X(t)$ in time Poly(g, n) for fixed p.
  (generalised by Tuitman to curves with separable map to $\mathbb{P}^1$)

Point counting & ℓ-torsion

p-adic point counting :

- ◇ Kedlaya (2001): given genus g hyperelliptic curve X over $\mathbb{F}_{p^n}$, computes zeta function $Z_X(t)$ in time Poly(g, n) for fixed p.
  (generalised by Tuitman to curves with separable map to $\mathbb{P}^1$)
- ◇ Harvey (2014): given suitable degree $2g+1$ polynomial f in $\mathbb{Z}[x]$, computes zeta function of corresponding hyperelliptic curve over $\mathbb{F}_p$ in time Poly$(\log(p), g)$ on average over p up to a given bound.

Point counting & ℓ-torsion

p-adic point counting :

- ◇ Kedlaya (2001): given genus g hyperelliptic curve X over $\mathbb{F}_{p^n}$, computes zeta function $Z_X(t)$ in time $\mathrm{Poly}(g, n)$ for fixed p.
  (generalised by Tuitman to curves with separable map to $\mathbb{P}^1$)
- ◇ Harvey (2014): given suitable degree $2g+1$ polynomial f in $\mathbb{Z}[x]$, computes zeta function of corresponding hyperelliptic curve over $\mathbb{F}_p$ in time $\mathrm{Poly}(\log(p), g)$ on average over p up to a given bound.

From point counting to torsion points in the Jacobian:

- ◇ Couveignes (2009): given smooth projective genus g curve X defined by $f \in \mathbb{F}_q[x, y]_d$ and its zeta function, computes $J_X[\ell]$ in time $\mathrm{Poly}(\ell, d, \log q, g)$

Projective curves: good complexity

Let X be a smooth projective curve over $\overline{\mathbb{F}_p}$. Let $Y \to X$ be an étale Galois covering, and M an $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module. Assume all of this comes from $\mathbb{F}_p$.

Projective curves: good complexity

Let X be a smooth projective curve over $\overline{\mathbb{F}_p}$. Let $Y \to X$ be an étale Galois covering, and M an $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module. Assume all of this comes from $\mathbb{F}_p$.

Algorithm (L.): compute $\mathrm{H}^1(X, M)$

- Compute the zeta function Z_Y of Y
- Determine large enough extension $\mathbb{F}_Q$ of $\mathbb{F}_p$
- Use Couveignes' algorithm to compute $J_Y[\ell](\mathbb{F}_Q)$ and $Y_D^{\langle \ell \rangle}$
- Compute $G = \mathrm{Aut}(Y_D^{\langle \ell \rangle}|X)$ and $\mathrm{H}^1(G, M)$

Projective curves: good complexity

Let X be a smooth projective curve over $\overline{\mathbb{F}_p}$. Let $Y \to X$ be an étale Galois covering, and M an $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module. Assume all of this comes from $\mathbb{F}_p$.

Algorithm (L.): compute $\mathrm{H}^1(X, M)$

- Compute the zeta function Z_Y of Y
- Determine large enough extension $\mathbb{F}_Q$ of $\mathbb{F}_p$
- Use Couveignes' algorithm to compute $J_Y[\ell](\mathbb{F}_Q)$ and $Y_D^{\langle \ell \rangle}$
- Compute $G = \mathrm{Aut}(Y_D^{\langle \ell \rangle}|X)$ and $\mathrm{H}^1(G, M)$

Complexity

Once Z_Y is known: $\mathrm{Poly}\left((\log(q), g_Y, \ell^{gx \dim_{\mathbb{F}_\ell}(M)}\right)$

Projective curves: good complexity

Let X be a smooth projective curve over $\overline{\mathbb{F}_p}$. Let $Y \to X$ be an étale Galois covering, and M an $\mathbb{F}_\ell[\mathrm{Aut}(Y|X)]$-module. Assume all of this comes from $\mathbb{F}_p$.

Algorithm (L.): compute $\mathrm{H}^1(X, M)$

- Compute the zeta function Z_Y of Y
- Determine large enough extension $\mathbb{F}_Q$ of $\mathbb{F}_p$
- Use Couveignes' algorithm to compute $J_Y[\ell](\mathbb{F}_Q)$ and $Y_D^{\langle \ell \rangle}$
- Compute $G = \mathrm{Aut}(Y_D^{\langle \ell \rangle}|X)$ and $\mathrm{H}^1(G, M)$

Complexity

Once Z_Y is known: $\mathrm{Poly}\left((\log(q), g_Y, \ell^{g_X \dim_{\mathbb{F}_\ell}(M)}\right)$

$\longrightarrow$ "the right one" (especially for hyperelliptic curves)

π_1-modules

The general method

Applying it to hyperelliptic curves

Practical solutions (even for affine curves)

Example (1/3)

- $p = 11, \ell = 2$

Example (1/3)

- $p = 11$, $\ell = 2$
- $E \mid y^2 = (x-1)(x-2)(x-3)$ elliptic curve
- $C \mid y^2 = (x^2-1)(x^2-2)(x^2-3)$ genus 2 curve
- $\bar{f} \colon C \to E, (x, y) \mapsto (x^2, y)$ ramified at $P = (0, 4)$, $Q = (0, 7)$

Example (1/3)

- $p = 11$, $\ell = 2$
- $E \mid y^2 = (x-1)(x-2)(x-3)$ elliptic curve
- $C \mid y^2 = (x^2-1)(x^2-2)(x^2-3)$ genus 2 curve
- $\bar{f} \colon C \to E, (x, y) \mapsto (x^2, y)$ ramified at $P = (0, 4)$, $Q = (0, 7)$
- $Y = C - \{P, Q\}$
- Compute $W = Y_D^{\langle \ell \rangle}$ and $\mathrm{Aut}(W|X)$

Example (2/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $Y = C - \{P, Q\}$

Example (2/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $Y = C - \{P, Q\}$
- Points of C with $y = 0$:
  $P_1^{\pm} = (\pm 1, 0)$, $P_2^{\pm} = (\pm\alpha^6, 0)$, $P_3^{\pm} = (\pm 5, 0)$ where $\alpha^2 + 7\alpha + 2 = 0$
- Basis of $\mathrm{H}^1(C, \mu_\ell)$:
  $D_1 = P_1^+ - P_1^-$, $D_2 = P_2^+ - P_2^-$, $D_3 = P_2^+ - P_3^+$, $D_4 = P_1^+ - P_3^-$

Example (2/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $Y = C - \{P, Q\}$
- Points of C with $y = 0$:
  $P_1^{\pm} = (\pm 1, 0)$, $P_2^{\pm} = (\pm\alpha^6, 0)$, $P_3^{\pm} = (\pm 5, 0)$ where $\alpha^2 + 7\alpha + 2 = 0$
- Basis of $\mathrm{H}^1(C, \mu_\ell)$:
  $D_1 = P_1^+ - P_1^-$, $D_2 = P_2^+ - P_2^-$, $D_3 = P_2^+ - P_3^+$, $D_4 = P_1^+ - P_3^-$
- Compute functions f_i s.t. $\mathrm{div}(f_i) = 2D_i$; eg $f_1 = \frac{x-1}{x+1}$

Example (2/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $Y = C - \{P, Q\}$
- Points of C with $y = 0$:
  $P_1^{\pm} = (\pm 1, 0)$, $P_2^{\pm} = (\pm \alpha^6, 0)$, $P_3^{\pm} = (\pm 5, 0)$ where $\alpha^2 + 7\alpha + 2 = 0$
- Basis of $\mathrm{H}^1(C, \mu_\ell)$:
  $D_1 = P_1^+ - P_1^-$, $D_2 = P_2^+ - P_2^-$, $D_3 = P_2^+ - P_3^+$, $D_4 = P_1^+ - P_3^-$
- Compute functions f_i s.t. $\mathrm{div}(f_i) = 2D_i$; eg $f_1 = \frac{x-1}{x+1}$
- One more element for a basis of $H^1(Y, \mu_\ell)$: find (D_5, f_5) s.t.
  $2D_5 = \mathrm{div}(f_5) + P - Q$.

Example (2/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $Y = C - \{P, Q\}$
- Points of C with $y = 0$:
  $P_1^{\pm} = (\pm 1, 0)$, $P_2^{\pm} = (\pm\alpha^6, 0)$, $P_3^{\pm} = (\pm 5, 0)$ where $\alpha^2 + 7\alpha + 2 = 0$
- Basis of $\mathrm{H}^1(C, \mu_\ell)$:
  $D_1 = P_1^+ - P_1^-$, $D_2 = P_2^+ - P_2^-$, $D_3 = P_2^+ - P_3^+$, $D_4 = P_1^+ - P_3^-$
- Compute functions f_i s.t. $\mathrm{div}(f_i) = 2D_i$; eg $f_1 = \frac{x-1}{x+1}$
- One more element for a basis of $H^1(Y, \mu_\ell)$: find (D_5, f_5) s.t.
  $2D_5 = \mathrm{div}(f_5) + P - Q$.
  $D_5 = (\alpha^{41}, \alpha^{29}) + (-\alpha^{41}, \alpha^{29}) - \infty_- - \infty_+$
  $2D_5 = P - Q + \mathrm{div}(f_5)$ where $f_5 = \frac{y + \alpha^8 x^2 + 7}{x}$

Example (2/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $Y = C - \{P, Q\}$
- Points of C with $y = 0$:
  $P_1^{\pm} = (\pm 1, 0)$, $P_2^{\pm} = (\pm\alpha^6, 0)$, $P_3^{\pm} = (\pm 5, 0)$ where $\alpha^2 + 7\alpha + 2 = 0$
- Basis of $\mathrm{H}^1(C, \mu_\ell)$:
  $D_1 = P_1^+ - P_1^-$, $D_2 = P_2^+ - P_2^-$, $D_3 = P_2^+ - P_3^+$, $D_4 = P_1^+ - P_3^-$
- Compute functions f_i s.t. $\mathrm{div}(f_i) = 2D_i$; eg $f_1 = \frac{x-1}{x+1}$
- One more element for a basis of $H^1(Y, \mu_\ell)$: find (D_5, f_5) s.t.
  $2D_5 = \mathrm{div}(f_5) + P - Q$.
  $D_5 = (\alpha^{41}, \alpha^{29}) + (-\alpha^{41}, \alpha^{29}) - \infty_- - \infty_+$
  $2D_5 = P - Q + \mathrm{div}(f_5)$ where $f_5 = \frac{y + \alpha^8 x^2 + 7}{x}$
- Basis of $H^1(Y, \mu_\ell)$: $(f_1, \ldots, f_5)$

Example (2/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $Y = C - \{P, Q\}$
- Points of C with $y = 0$:
  $P_1^{\pm} = (\pm 1, 0)$, $P_2^{\pm} = (\pm\alpha^6, 0)$, $P_3^{\pm} = (\pm 5, 0)$ where $\alpha^2 + 7\alpha + 2 = 0$
- Basis of $\mathrm{H}^1(C, \mu_\ell)$:
  $D_1 = P_1^+ - P_1^-$, $D_2 = P_2^+ - P_2^-$, $D_3 = P_2^+ - P_3^+$, $D_4 = P_1^+ - P_3^-$
- Compute functions f_i s.t. $\mathrm{div}(f_i) = 2D_i$; eg $f_1 = \frac{x-1}{x+1}$
- One more element for a basis of $H^1(Y, \mu_\ell)$: find (D_5, f_5) s.t.
  $2D_5 = \mathrm{div}(f_5) + P - Q$.
  $D_5 = (\alpha^{41}, \alpha^{29}) + (-\alpha^{41}, \alpha^{29}) - \infty_- - \infty_+$
  $2D_5 = P - Q + \mathrm{div}(f_5)$ where $f_5 = \frac{y + \alpha^8 x^2 + 7}{x}$
- Basis of $H^1(Y, \mu_\ell)$: $(f_1, \ldots, f_5)$
- $k(W) = k(Y)(z_1, \ldots, z_5)$ where $z_i = \sqrt[\ell]{f_i}$

Example (3/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $f\colon Y \to X$, where $Y = C - \{P, Q\}$, $\mathrm{Aut}(Y|X) = \langle \sigma\colon x \mapsto -x \rangle$

Example (3/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $f\colon Y \to X$, where $Y = C - \{P, Q\}$, $\mathrm{Aut}(Y|X) = \langle \sigma\colon x \mapsto -x \rangle$
- $k(W) = k(Y)(z_1, \ldots, z_5)$ where $z_i = \sqrt[\ell]{f_i}$
- $\mathrm{Aut}(W|Y) \simeq (\mathbb{Z}/2\mathbb{Z})^5 \subset \mathrm{Aut}(W|X)$

Example (3/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $f\colon Y \to X$, where $Y = C - \{P, Q\}$, $\mathrm{Aut}(Y|X) = \langle \sigma\colon x \mapsto -x \rangle$
- $k(W) = k(Y)(z_1, \ldots, z_5)$ where $z_i = \sqrt[\ell]{f_i}$
- $\mathrm{Aut}(W|Y) \simeq (\mathbb{Z}/2\mathbb{Z})^5 \subset \mathrm{Aut}(W|X)$
- Find a preimage of σ in $\mathrm{Aut}(W|X)$: $\sigma^\star D_1 = -D_1$, $\sigma^\star D_2 = -D_2$,

Example (3/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $f\colon Y \to X$, where $Y = C - \{P, Q\}$, $\mathrm{Aut}(Y|X) = \langle \sigma\colon x \mapsto -x \rangle$
- $k(W) = k(Y)(z_1, \ldots, z_5)$ where $z_i = \sqrt[\ell]{f_i}$
- $\mathrm{Aut}(W|Y) \simeq (\mathbb{Z}/2\mathbb{Z})^5 \subset \mathrm{Aut}(W|X)$
- Find a preimage of σ in $\mathrm{Aut}(W|X)$: $\sigma^\star D_1 = -D_1$, $\sigma^\star D_2 = -D_2$,
  $\sigma^\star D_3 = D_1 + D_3 + \mathrm{div}(h_3)$ where $h_3 = \frac{y}{x^3+\alpha^{58}x^2+\alpha^2 x+\alpha^{54}}$
  $\sigma^\star D_4 = D_2 + D_4 + \mathrm{div}(h_4)$ where $h_4 = \frac{y}{x^3+\alpha^{80}x^2+\alpha^{103}x+\alpha^{114}}$

Example (3/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $f\colon Y \to X$, where $Y = C - \{P, Q\}$, $\mathrm{Aut}(Y|X) = \langle \sigma\colon x \mapsto -x \rangle$
- $k(W) = k(Y)(z_1, \ldots, z_5)$ where $z_i = \sqrt[\ell]{f_i}$
- $\mathrm{Aut}(W|Y) \simeq (\mathbb{Z}/2\mathbb{Z})^5 \subset \mathrm{Aut}(W|X)$
- Find a preimage of σ in $\mathrm{Aut}(W|X)$: $\sigma^\star D_1 = -D_1$, $\sigma^\star D_2 = -D_2$,
  $\sigma^\star D_3 = D_1 + D_3 + \mathrm{div}(h_3)$ where $h_3 = \frac{y}{x^3 + \alpha^{58} x^2 + \alpha^2 x + \alpha^{54}}$
  $\sigma^\star D_4 = D_2 + D_4 + \mathrm{div}(h_4)$ where $h_4 = \frac{y}{x^3 + \alpha^{80} x^2 + \alpha^{103} x + \alpha^{114}}$
  $\sigma^\star D_5 = D_5$ (and actually $\sigma^\star f_5 = -f_5$)

Example (3/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $f\colon Y \to X$, where $Y = C - \{P, Q\}$, $\mathrm{Aut}(Y|X) = \langle \sigma\colon x \mapsto -x \rangle$
- $k(W) = k(Y)(z_1, \ldots, z_5)$ where $z_i = \sqrt[\ell]{f_i}$
- $\mathrm{Aut}(W|Y) \simeq (\mathbb{Z}/2\mathbb{Z})^5 \subset \mathrm{Aut}(W|X)$
- Find a preimage of σ in $\mathrm{Aut}(W|X)$: $\sigma^\star D_1 = -D_1$, $\sigma^\star D_2 = -D_2$,
  $\sigma^\star D_3 = D_1 + D_3 + \mathrm{div}(h_3)$ where $h_3 = \frac{y}{x^3 + \alpha^{58}x^2 + \alpha^2 x + \alpha^{54}}$
  $\sigma^\star D_4 = D_2 + D_4 + \mathrm{div}(h_4)$ where $h_4 = \frac{y}{x^3 + \alpha^{80}x^2 + \alpha^{103}x + \alpha^{114}}$
  $\sigma^\star D_5 = D_5$ (and actually $\sigma^\star f_5 = -f_5$)
- $\sigma'\colon x \mapsto -x, \quad y \mapsto y,$
  $z_1 \mapsto \frac{1}{z_1}, \quad z_2 \mapsto \frac{1}{z_2}, \quad z_3 \mapsto h_3(x,y) z_1 z_3, \quad z_4 \mapsto h_4(x,y) z_2 z_4, \quad z_5 \mapsto \sqrt{-1} z_5$

Example (3/3)

- $p = 11$, $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, $\ell = 2$
- $f\colon Y \to X$, where $Y = C - \{P, Q\}$, $\mathrm{Aut}(Y|X) = \langle \sigma\colon x \mapsto -x \rangle$
- $k(W) = k(Y)(z_1, \ldots, z_5)$ where $z_i = \sqrt[\ell]{f_i}$
- $\mathrm{Aut}(W|Y) \simeq (\mathbb{Z}/2\mathbb{Z})^5 \subset \mathrm{Aut}(W|X)$
- Find a preimage of σ in $\mathrm{Aut}(W|X)$: $\sigma^\star D_1 = -D_1$, $\sigma^\star D_2 = -D_2$,
  $\sigma^\star D_3 = D_1 + D_3 + \mathrm{div}(h_3)$ where $h_3 = \frac{y}{x^3 + \alpha^{58}x^2 + \alpha^2 x + \alpha^{54}}$
  $\sigma^\star D_4 = D_2 + D_4 + \mathrm{div}(h_4)$ where $h_4 = \frac{y}{x^3 + \alpha^{80}x^2 + \alpha^{103}x + \alpha^{114}}$
  $\sigma^\star D_5 = D_5$ (and actually $\sigma^\star f_5 = -f_5$)
- $\sigma'\colon x \mapsto -x, \quad y \mapsto y,$
  $z_1 \mapsto \frac{1}{z_1}, \quad z_2 \mapsto \frac{1}{z_2}, \quad z_3 \mapsto h_3(x,y) z_1 z_3, \quad z_4 \mapsto h_4(x,y) z_2 z_4, \quad z_5 \mapsto \sqrt{-1} z_5$
- $\mathrm{Aut}(W|X) = \sigma' \cdot \mathrm{Aut}(W|Y)$ has order $2 \times 2^5 = 64$

Division by ℓ in practice

Let X be a hyperelliptic curve defined by $y^2 = f(x)$, where $\deg(f) = 2g + 1$. Denote by $\alpha_1, \ldots, \alpha_{2g+1}$ the roots of f.

Division by ℓ in practice

Let X be a hyperelliptic curve defined by $y^2 = f(x)$, where $\deg(f) = 2g + 1$.
Denote by $\alpha_1, \ldots, \alpha_{2g+1}$ the roots of f.
Given $P = (a, b) \in X$, find D such that $\ell[D] = [P - \infty]$.

- ◇ When g is small: use division polynomials over hyperelliptic curves.
  Given $P - \infty$, take indeterminate points $P_1 = (a_1, b_1), \ldots, P_g = (a_g, b_g)$,
  compute $S = [\ell P_1 + \cdots + \ell P_g - g\infty]$ (yields divisor depending on a_i, b_i)

Division by ℓ in practice

Let X be a hyperelliptic curve defined by $y^2 = f(x)$, where $\deg(f) = 2g + 1$.
Denote by $\alpha_1, \ldots, \alpha_{2g+1}$ the roots of f.
Given $P = (a, b) \in X$, find D such that $\ell[D] = [P - \infty]$.

- ◇ When g is small: use division polynomials over hyperelliptic curves.
  Given $P - \infty$, take indeterminate points $P_1 = (a_1, b_1), \ldots, P_g = (a_g, b_g)$, compute $S = [\ell P_1 + \cdots + \ell P_g - g\infty]$ (yields divisor depending on a_i, b_i) and solve system $S = [P - \infty] \longrightarrow$ Gröbner bases

Division by ℓ in practice

Let X be a hyperelliptic curve defined by $y^2 = f(x)$, where $\deg(f) = 2g + 1$.
Denote by $\alpha_1, \ldots, \alpha_{2g+1}$ the roots of f.
Given $P = (a, b) \in X$, find D such that $\ell[D] = [P - \infty]$.

- ◇ When g is small: use division polynomials over hyperelliptic curves. Given $P - \infty$, take indeterminate points $P_1 = (a_1, b_1), \ldots, P_g = (a_g, b_g)$, compute $S = [\ell P_1 + \cdots + \ell P_g - g\infty]$ (yields divisor depending on a_i, b_i) and solve system $S = [P - \infty] \longrightarrow$ Gröbner bases
- ◇ When $\ell = 2$: Zarhin's thm shows that the set of suitable $[D]$ is in (explicit) bijection with tuples $(r_1, \ldots, r_{2g+1})$ such that $r_i^2 = a - \alpha_i$ and $r_1 \cdots r_{2g+1} = -b$

Implementation

- Implementation in progress for (affine opens of) hyperelliptic covers

Implementation

- Implementation in progress for (affine opens of) hyperelliptic covers
- Will also work for constructible sheaves

Implementation

- Implementation in progress for (affine opens of) hyperelliptic covers
- Will also work for constructible sheaves
- Easy for $\ell = 2$, $g = 2$

Implementation

- Implementation in progress for (affine opens of) hyperelliptic covers
- Will also work for constructible sheaves
- Easy for $\ell = 2$, $g = 2$
- For one covering $Y \to X$, computing $Y_D^{\langle \ell \rangle}$ once allows to compute the cohomology of any $\pi_1(X)$-module of given $\mathbb{F}_\ell$-dimension trivialised by Y

Implementation

- ◇ Implementation in progress for (affine opens of) hyperelliptic covers
- ◇ Will also work for constructible sheaves
- ◇ Easy for $\ell = 2$, $g = 2$
- ◇ For one covering $Y \to X$, computing $Y_D^{\langle \ell \rangle}$ once allows to compute the cohomology of any $\pi_1(X)$-module of given $\mathbb{F}_\ell$-dimension trivialised by Y
- ◇ Computing preimages in $\mathrm{Aut}(Y_D^{\langle \ell \rangle} | X)$ of $\sigma \in \mathrm{Aut}(Y|X)$: first action of σ on divisor classes of $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q)$, then on functions

Implementation

- Implementation in progress for (affine opens of) hyperelliptic covers
- Will also work for constructible sheaves
- Easy for $\ell = 2$, $g = 2$
- For one covering $Y \to X$, computing $Y_D^{\langle \ell \rangle}$ once allows to compute the cohomology of any $\pi_1(X)$-module of given $\mathbb{F}_\ell$-dimension trivialised by Y
- Computing preimages in $\mathrm{Aut}(Y_D^{\langle \ell \rangle} | X)$ of $\sigma \in \mathrm{Aut}(Y|X)$: first action of σ on divisor classes of $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q)$, then on functions
- Don't automatically base change to $\mathbb{F}_Q$ (previous example)

Implementation

- Implementation in progress for (affine opens of) hyperelliptic covers
- Will also work for constructible sheaves
- Easy for $\ell = 2$, $g = 2$
- For one covering $Y \to X$, computing $Y_D^{\langle \ell \rangle}$ once allows to compute the cohomology of any $\pi_1(X)$-module of given $\mathbb{F}_\ell$-dimension trivialised by Y
- Computing preimages in $\mathrm{Aut}(Y_D^{\langle \ell \rangle} | X)$ of $\sigma \in \mathrm{Aut}(Y|X)$: first action of σ on divisor classes of $\mathrm{H}^1(Y, \mu_\ell)(\mathbb{F}_Q)$, then on functions
- Don't automatically base change to $\mathbb{F}_Q$ (previous example)
- Magma is your (sometimes mysterious) friend!

Thank you!