Computing twists of hyperelliptic curves

ICTP Workshop on Hyperelliptic Curves

Davide Lombardo

(joint with E. Lorenzo-García)

Università di Pisa

07 September 2017

What's a hyperelliptic curve, really?

What's a hyperelliptic curve, really?

Definition

A (smooth, projective, geometrically connected) curve C over a field K is **hyperelliptic** if the canonical map is a 2-to-1 cover $C \to Q$ with Q of genus 0.

What's a hyperelliptic curve, really?

Definition

A (smooth, projective, geometrically connected) curve C over a field K is **hyperelliptic** if the canonical map is a 2-to-1 cover $C \to Q$ with Q of genus 0.

Remark (char$(K) = 0$)

If $Q(K) \neq \emptyset$, then $Q \cong \mathbb{P}^1_K$ and C admits a K-model of the form $y^2 = f(x)$.

What's a hyperelliptic curve, really?

Definition

A (smooth, projective, geometrically connected) curve C over a field K is **hyperelliptic** if the canonical map is a 2-to-1 cover $C \to Q$ with Q of genus 0.

Remark ($\mathrm{char}(K) = 0$)

If $Q(K) \neq \emptyset$, then $Q \cong \mathbb{P}^1_K$ and C admits a K-model of the form $y^2 = f(x)$. Otherwise, g is odd and C has a model of the form

$$C : \begin{cases} aX^2 + bY^2 + cZ^2 = 0 \\ t^2 = f(X, Y, Z) \end{cases} \quad \subset \mathbb{P}_{1,1,1,\frac{g+1}{2}}(K)$$

Twists of curves

A **twist** of a curve C/K is another curve C'/K such that $C_{\overline{K}} \sim C'_{\overline{K}}$.

Twists of curves

A **twist** of a curve C/K is another curve C'/K such that $C_{\overline{K}} \sim C'_{\overline{K}}$.

Theorem

There is a one-to-one correspondence

$$\text{Twists}(C/K)/\{K - isomorphism\} \longleftrightarrow H^1(\Gamma_K, \text{Aut}_{\overline{K}}(C))$$

Twists of curves
II

How does the correspondence work?

Twists of curves
II

How does the correspondence work?

If $C \xrightarrow{\varphi} C'$ is a $\overline{K}$-isomorphism, the corresponding cohomology class is represented by

$$\begin{array}{rccc} \xi : & \Gamma_K & \to & \mathrm{Aut}_{\overline{K}}(C) \\ & \sigma & \mapsto & {}^{\sigma}(\varphi^{-1}) \circ \varphi \end{array}$$

Twists of curves
II

How does the correspondence work?

If $C \xrightarrow{\varphi} C'$ is a $\overline{K}$-isomorphism, the corresponding cohomology class is represented by

$$\begin{array}{rccc} \xi: & \Gamma_K & \to & \mathrm{Aut}_{\overline{K}}(C) \\ & \sigma & \mapsto & {}^{\sigma}(\varphi^{-1}) \circ \varphi \end{array}$$

What about the other arrow, $\xi \mapsto C^{\xi}$?

How does the correspondence work?

If $C \xrightarrow{\varphi} C'$ is a $\overline{K}$-isomorphism, the corresponding cohomology class is represented by

$$\begin{array}{rccc} \xi : & \Gamma_K & \to & \mathrm{Aut}_{\overline{K}}(C) \\ & \sigma & \mapsto & {}^{\sigma}(\varphi^{-1}) \circ \varphi \end{array}$$

What about the other arrow, $\xi \mapsto C^{\xi}$? There's a recipe, but...

How does the correspondence work?

If $C \xrightarrow{\varphi} C'$ is a $\overline{K}$-isomorphism, the corresponding cohomology class is represented by

$$\begin{array}{rccc} \xi : & \Gamma_K & \to & \mathrm{Aut}_{\overline{K}}(C) \\ & \sigma & \mapsto & {}^{\sigma}(\varphi^{-1}) \circ \varphi \end{array}$$

What about the other arrow, $\xi \mapsto C^{\xi}$? There's a recipe, but...

Example

Using this naïve approach, MAGMA was unable to find a planar model for

$$C^{\xi} : y^2 = -x^8 + 4x^7 - 28x^6 + 28x^5 + 14x^4 + 28x^3 - 196x^2 + 100x - 61$$

Twisting non-hyperelliptic curves

I

Given C/K non-hyperelliptic (of genus ≥ 3), there is a canonical embedding

$$C \hookrightarrow \mathbb{P}H^0\left(C, \Omega_C^1\right) \cong \mathbb{P}_K^{g-1}.$$

Twisting non-hyperelliptic curves

I

Given C/K non-hyperelliptic (of genus ≥ 3), there is a canonical embedding

$$C \hookrightarrow \mathbb{P}H^0\left(C, \Omega^1_C\right) \cong \mathbb{P}^{g-1}_K.$$

The automorphism group of C acts (by pullback) on the space of regular differentials on C

Twisting non-hyperelliptic curves

Given C/K non-hyperelliptic (of genus ≥ 3), there is a canonical embedding
$$C \hookrightarrow \mathbb{P}H^0\left(C, \Omega^1_C\right) \cong \mathbb{P}^{g-1}_K.$$

The automorphism group of C acts (by pullback) on the space of regular differentials on C $\rightsquigarrow$ we have a Galois-equivariant embedding of $\mathrm{Aut}_{\overline{K}}(C)$ in $\mathrm{GL}(H^0\left(C_{\overline{K}}, \Omega^1_C\right)) \cong \mathrm{GL}_g(\overline{K})$

Twisting non-hyperelliptic curves

II

Suppose given a non-hyperelliptic curve C/K (of genus ≥ 3) and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$.

Twisting non-hyperelliptic curves
II

Suppose given a non-hyperelliptic curve C/K (of genus ≥ 3) and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$. Composing with $\mathrm{Aut}_{\overline{K}}(C) \hookrightarrow \mathrm{GL}_g(\overline{K})$, we obtain a cocycle

$$\xi_L : \Gamma_K \to \mathrm{GL}_g(\overline{K})$$

Twisting non-hyperelliptic curves

II

Suppose given a non-hyperelliptic curve C/K (of genus ≥ 3) and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$. Composing with $\mathrm{Aut}_{\overline{K}}(C) \hookrightarrow \mathrm{GL}_g(\overline{K})$, we obtain a cocycle

$$\xi_L : \Gamma_K \to \mathrm{GL}_g(\overline{K})$$

Algorithm

- By Hilbert 90, there exists $M \in \mathrm{GL}_g(\overline{K})$ such that

$$\xi_L(\sigma) = {}^{\sigma}(M^{-1}) \cdot M.$$

Twisting non-hyperelliptic curves

II

Suppose given a non-hyperelliptic curve C/K (of genus ≥ 3) and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$. Composing with $\mathrm{Aut}_{\overline{K}}(C) \hookrightarrow \mathrm{GL}_g(\overline{K})$, we obtain a cocycle

$$\xi_L : \Gamma_K \to \mathrm{GL}_g(\overline{K})$$

Algorithm

- By Hilbert 90, there exists $M \in \mathrm{GL}_g(\overline{K})$ such that

$$\xi_L(\sigma) = {}^{\sigma}(M^{-1}) \cdot M.$$

- M induces a linear map $[M] : \mathbb{P}^{g-1}_{\overline{K}} \to \mathbb{P}^{g-1}_{\overline{K}}$.

Twisting non-hyperelliptic curves
II

Suppose given a non-hyperelliptic curve C/K (of genus ≥ 3) and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$. Composing with $\mathrm{Aut}_{\overline{K}}(C) \hookrightarrow \mathrm{GL}_g(\overline{K})$, we obtain a cocycle

$$\xi_L : \Gamma_K \to \mathrm{GL}_g(\overline{K})$$

Algorithm

- By Hilbert 90, there exists $M \in \mathrm{GL}_g(\overline{K})$ such that

$$\xi_L(\sigma) = {}^{\sigma}(M^{-1}) \cdot M.$$

- M induces a linear map $[M] : \mathbb{P}^{g-1}_{\overline{K}} \to \mathbb{P}^{g-1}_{\overline{K}}$.
- The image $[M](C)$ is a curve defined over K; from this, one easily obtains equations for C^{ξ}.

The hyperelliptic case

Suppose given a hyperelliptic curve C/K of genus $g \geq 2$ and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$.

The hyperelliptic case

Suppose given a hyperelliptic curve C/K of genus $g \geq 2$ and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$.

One can try to mimic the non-hyperelliptic case by embedding C in projective space via higher powers of the canonical bundle.

The hyperelliptic case

Suppose given a hyperelliptic curve C/K of genus $g \geq 2$ and a cocycle $\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$.

One can try to mimic the non-hyperelliptic case by embedding C in projective space via higher powers of the canonical bundle. This can be computationally expensive ($H^0(C, (\Omega^1_C)^{\otimes 2})$ has dimension $3(g-1)$).

The hyperelliptic case
II

Input data

$$C : \begin{cases} aX^2 + bY^2 + cZ^2 = 0 \\ t^2 = f(X, Y, Z) \end{cases} \quad \leftrightsquigarrow \quad Q(X, Y, Z) = 0$$

The hyperelliptic case

II

Input data

$$C : \begin{cases} aX^2 + bY^2 + cZ^2 = 0 & \leftrightsquigarrow \quad Q(X, Y, Z) = 0 \\ t^2 = f(X, Y, Z) \end{cases}$$

$$\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C)$$

The hyperelliptic case
II

Input data

$$C : \begin{cases} aX^2 + bY^2 + cZ^2 = 0 & \leftrightsquigarrow \quad Q(X, Y, Z) = 0 \\ t^2 = f(X, Y, Z) \end{cases}$$

$$\xi : \Gamma_K \to \mathrm{Aut}_{\overline{K}}(C) \to \mathrm{Aut}_{\overline{K}}(Q)$$

The hyperelliptic case

III

1. Using the **anti-canonical** model of Q, embed $\mathrm{Aut}_{\overline{K}}(Q)$ into $\mathrm{GL}_3(\overline{K})$

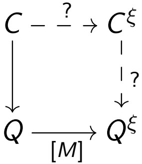
The hyperelliptic case

III

1. Using the **anti-canonical** model of Q, embed $\mathrm{Aut}_{\overline{K}}(Q)$ into $\mathrm{GL}_3(\overline{K})$
2. Apply Hilbert 90 to split the cocycle, $\xi_L(\sigma) = {}^{\sigma}(M^{-1}) \cdot M$.

The hyperelliptic case
III

1. Using the **anti-canonical** model of Q, embed $\mathrm{Aut}_{\overline{K}}(Q)$ into $\mathrm{GL}_3(\overline{K})$
2. Apply Hilbert 90 to split the cocycle, $\xi_L(\sigma) = {}^{\sigma}(M^{-1}) \cdot M$.
3. In this way we obtain $Q^{\xi}(X, Y, Z) = Q(M(X, Y, Z))$, which fits into



The hyperelliptic case

III

1. Using the **anti-canonical** model of Q, embed $\mathrm{Aut}_{\overline{K}}(Q)$ into $\mathrm{GL}_3(\overline{K})$
2. Apply Hilbert 90 to split the cocycle, $\xi_L(\sigma) = {}^{\sigma}(M^{-1}) \cdot M$.
3. In this way we obtain $Q^{\xi}(X, Y, Z) = Q(M(X, Y, Z))$, which fits into

$$\begin{array}{ccc} C & \overset{?}{\dashrightarrow} & C^{\xi} \\ \big\downarrow & & \big\downarrow{?} \\ Q & \underset{[M]}{\longrightarrow} & Q^{\xi} \end{array}$$

4. First guess:

$$C : \begin{cases} Q(X, Y, Z) = 0 \\ t^2 = F(X, Y, Z) \end{cases} \quad \to C' : \begin{cases} Q(M(X, Y, Z)) = 0 \\ t^2 = F(M(X, Y, Z)) \end{cases}$$

The hyperelliptic case
IV

First guess:

$$C' : \begin{cases} Q(M(X,Y,Z)) = 0 \\ t^2 = F(M(X,Y,Z)) \end{cases}$$

The hyperelliptic case
IV

First guess:

$$C' : \begin{cases} Q(M(X,Y,Z)) = 0 \\ t^2 = F(M(X,Y,Z)) \end{cases}$$

Theorem (L. – Lorenzo-García)

There exist $\lambda \in \overline{K}^{\times}$, a finite extension L/K containing the coefficients of $\lambda F(M(X,Y,Z))$, and an element $e \in K^{\times}$ such that a K-model of C^{ξ} is given by

$$\begin{cases} Q(M(X,Y,Z)) = 0 \\ et^2 = \frac{1}{[L:K]} \operatorname{tr}_{L/K}(\lambda F(M(X,Y,Z))) \end{cases}$$

where the trace is taken coefficientwise.

The hyperelliptic case

IV

First guess:

$$C' : \begin{cases} Q(M(X,Y,Z)) = 0 \\ t^2 = F(M(X,Y,Z)) \end{cases}$$

Theorem (L. – Lorenzo-García)

There exist $\lambda \in \overline{K}^\times$, a finite extension L/K containing the coefficients of $\lambda F(M(X,Y,Z))$, and an element $e \in K^\times$ such that a K-model of C^ξ is given by

$$\begin{cases} Q(M(X,Y,Z)) = 0 \\ et^2 = \frac{1}{[L:K]} \operatorname{tr}_{L/K}(\lambda F(M(X,Y,Z))) \end{cases}$$

where the trace is taken coefficientwise. λ, L and e are all easy to compute.

Example

Input

$$C : \begin{cases} X^2 + Y^2 + Z^2 = 0 \\ t^2 = X^4 + Y^4 + Z^4 \end{cases} \quad \subset \mathbb{P}_{1,1,1,2}(\mathbb{Q})$$

Example

Input

$$C : \begin{cases} X^2 + Y^2 + Z^2 = 0 \\ t^2 = X^4 + Y^4 + Z^4 \end{cases} \quad \subset \mathbb{P}_{1,1,1,2}(\mathbb{Q})$$

$$\begin{array}{rccc} \xi : & \mathrm{Gal}\left(\mathbb{Q}(\zeta_9)^+/\mathbb{Q}\right) = \langle \sigma \rangle & \rightarrow & \mathrm{Aut}_{\overline{\mathbb{Q}}}(C) \\ & \sigma & \mapsto & [X, Y, Z, t] \mapsto [Y, Z, X, t] \end{array}$$

Example

Input

$$C : \begin{cases} X^2 + Y^2 + Z^2 = 0 \\ t^2 = X^4 + Y^4 + Z^4 \end{cases} \subset \mathbb{P}_{1,1,1,2}(\mathbb{Q})$$

$$\begin{array}{llcl} \xi : & \mathrm{Gal}\left(\mathbb{Q}(\zeta_9)^+/\mathbb{Q}\right) = \langle \sigma \rangle & \to & \mathrm{Aut}_{\overline{\mathbb{Q}}}(C) \\ & \sigma & \mapsto & [X, Y, Z, t] \mapsto [Y, Z, X, t] \end{array}$$

Output

$$\begin{cases} X^2 + Y^2 + Z^2 = 0 \\ -3t^2 = -23(X^4 + Y^4 + Z^4) - 12XZ(XY + YZ + ZX + Y^2) \\ \qquad + 20(XY^3 + YZ^3 - ZX^3) + 16(XZ^3 - X^3Y - Y^3Z) \\ \qquad - 12Y^2(X^2 + Z^2) \end{cases}$$

Thank you!