New Magma functionality for curves of genus 2 and 3

Reynald Lercier
(Université de Rennes 1)

Christophe Ritzenthaler
(Université de Rennes 1, Université Côte d'Azur)

Jeroen Sijsling
(Universität Ulm)

MEGA 2021
University of Tromsø, June 7-11, 2021

Overview

Themes of the algorithms discussed in this talk:

- Hyperelliptic curves (isomorphisms and twists);
- Plane quartic curves (isomorphisms and twists);
- Invariants and reconstruction for hyperelliptic curves of genus 2 and 3;
- Invariants and reconstruction for plane quartics.

Corresponding functions have been added to Magma in V2.26.

Overview

Themes of the algorithms discussed in this talk:

- Hyperelliptic curves (isomorphisms and twists);
- Plane quartic curves (isomorphisms and twists);
- Invariants and reconstruction for hyperelliptic curves of genus 2 and 3;
- Invariants and reconstruction for plane quartics.

Corresponding functions have been added to Magma in V2.26.

All curves are smooth in this talk, and we fix a ground field k throughout.

Hyperelliptic curves: Definition

Definition

Let $\mathrm{char}(k) \neq 2$. A hyperelliptic curve over k is a curve C over k that over $\overline{k}$ admits a defining equation

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

where f is a separable polynomial in $\overline{k}[x]$.

Hyperelliptic curves: Definition

Definition

Let $\mathrm{char}(k) \neq 2$. A hyperelliptic curve over k is a curve C over k that over $\overline{k}$ admits a defining equation

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

where f is a separable polynomial in $\overline{k}[x]$.

Warning: In odd genus, there exist hyperelliptic curves over k for which no equation of the given form exists over k.

Hyperelliptic curves: Definition

Definition

Let $\mathrm{char}(k) \neq 2$. A hyperelliptic curve over k is a curve C over k that over $\overline{k}$ admits a defining equation

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

where f is a separable polynomial in $\overline{k}[x]$.

Warning: In odd genus, there exist hyperelliptic curves over k for which no equation of the given form exists over k.

While our algorithms in fact work with the specific defining equations above, they generalize unproblematically after finding a point on the conic covered by C over a quadratic extension of k.

Hyperelliptic curves: Isomorphisms

Proposition

Let $C_i : y^2 = f_i(x)$ be two hyperelliptic curves of genus g over k. Then any isomorphism $C_1 \to C_2$ is of the form

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^{g+1}} \right).$$

Hyperelliptic curves: Isomorphisms

Proposition

Let $C_i : y^2 = f_i(x)$ be two hyperelliptic curves of genus g over k. Then any isomorphism $C_1 \to C_2$ is of the form

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^{g+1}} \right).$$

Main method used to make this calculation tractable: covariants.

Hyperelliptic curves: Isomorphisms

Proposition

Let $C_i : y^2 = f_i(x)$ be two hyperelliptic curves over k. Then any isomorphism $C_1 \to C_2$ is of the form

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^{g+1}} \right).$$

- The new algorithms find isomorphisms quickly (average time over $\mathbb{F}^2_{10^{12}+39}$: 0.008 s, versus 0.917 s beforehand).
- Moreover, they determine the geometric isomorphisms $C_1 \to C_2$ (those defined over $\overline{k}$) as well.
- Format: `IsIsomorphicHyperellipticCurves(C1, C2 : geometric := true)`

Hyperelliptic curves: Twists

Definition

Let C be a curve over k. A twist of C is another curve C' over k with the property that

$$C \cong C' \text{ over } \overline{k}.$$

Given C, we determine the twists of C up to k-isomorphism.

Hyperelliptic curves: Twists

Definition

Let C be a curve over k. A twist of C is another curve C' over k with the property that

$$C \cong C' \text{ over } \overline{k}.$$

Given C, we determine the twists of C up to k-isomorphism.

Implementation for hyperelliptic curves (specific to finite fields):

- Calculate the automorphisms (A, e) of C over $\overline{k}$.
- Determine the Frobenius conjugacy classes of the reduced automorphism group generated by the matrices A.
- Twist using Hilbert 90 to get a new polynomial $f' \in k[x]$, and throw in the (one or two) corresponding curves.

Hyperelliptic curves: Twists

Definition

Let C be a curve over k. A twist of C is another curve C' over k with the property that

$$C \cong C' \text{ over } \overline{k}.$$

Given C, we determine the twists of C up to k-isomorphism.

Implementation for hyperelliptic curves (specific to finite fields):

- Calculate the automorphisms (A, e) of C over $\overline{k}$.
- Determine the Frobenius conjugacy classes of the reduced automorphism group generated by the matrices A.
- Twist using Hilbert 90 to get a new polynomial $f' \in k[x]$, and throw in the (one or two) corresponding curves.
- Alternative by Lombardo and Lorenzo García also available.
- Format: `Twists(C : AutomorphismGroup := true)`

Plane quartic curves: Definition

Definition

A plane quartic curve is a projective curve $C : F(x, y, z) = 0$ defined by a ternary quartic form F.

Proposition

Let $C_i : F_i(x, y, z) = 0$ be two plane quartic curves over k. Then any isomorphism $C_1 \to C_2$ is induced by an element $T \in \mathrm{PGL}_3(k)$ such that up to scalar

$$F_2 = F_1 \cdot T.$$

Plane quartic curves: Isomorphisms

Proposition

Let $C_i : F_i(x, y, z) = 0$ be two plane quartic curves over k. Then any isomorphism $C_1 \to C_2$ is induced by an element $T \in \mathrm{PGL}_3(k)$ such that up to scalar

$$F_2 = F_1 \cdot T.$$

- Determination of possible T using a ternary contravariant (idea due to Van Rijnswou) or by using hyperflexes or Groebner methods.

Plane quartic curves: Isomorphisms

Proposition

Let $C_i : F_i(x, y, z) = 0$ be two plane quartic curves over k. Then any isomorphism $C_1 \to C_2$ is induced by an element $T \in \mathrm{PGL}_3(k)$ such that up to scalar

$$F_2 = F_1 \cdot T.$$

- The new algorithms find isomorphisms quickly (average time over $\mathbb{F}^2_{10^6+3}$: 0.021 s, versus 7.233 s beforehand).
- We can again determine the geometric isomorphisms $C_1 \to C_2$, as long as k is a finite field or $\mathbb{Q}$.
- Format: `IsIsomorphicPlaneQuartics(C1, C2 : geometric := true)`
- Twists over finite fields can again be determined (same format).

Hyperelliptic curves: Invariants

Studying moduli of hyperelliptic curves for algebraically closed k is the same as studying the $\mathrm{GL}_2(k)$-orbits of binary forms

$$f(x,z) = z^{2g+2} f(x/z)$$

or in other words as studying the space

$$R_g(k) = \left(\bigoplus_{n \geq 0} \mathrm{Sym}^n(\mathrm{Sym}^{2g+2}(k^2)) \right)^{\mathrm{SL}_2(k)}.$$

Hyperelliptic curves: Invariants

Studying moduli of hyperelliptic curves for algebraically closed k is the same as studying the $\mathrm{GL}_2(k)$-orbits of binary forms

$$f(x,z) = z^{2g+2} f(x/z)$$

or in other words as studying the space

$$R_g(k) = \left(\bigoplus_{n \geq 0} \mathrm{Sym}^n(\mathrm{Sym}^{2g+2}(k^2)) \right)^{\mathrm{SL}_2(k)}.$$

For $g = 2$, we have Igusa invariants $I_2, I_4, I_6, I_8, I_{10}$ that work over any field.

For $g = 3$, we have Shioda invariants $S_2, \ldots S_{10}$ over $\mathbb{C}$. Their reductions also work if $\mathrm{char}(k) > 7$.

Hyperelliptic curves: Invariants

In genus 3, Romain Basson found separants for fields of arbitrary characteristic except 5. These are invariants $(B_1, \ldots, B_N)$ of weights $w = (w_1, \ldots, w_N)$ such that

$$f_1 \overset{\mathrm{GL}_2(\bar{k})}{\sim} f_2 \quad \Leftrightarrow \quad (B_i(f_1))_{i=1}^N = (B_i(f_2))_{i=1}^N \text{ in } \mathbb{P}^w.$$

Hyperelliptic curves: Invariants

In genus 3, Romain Basson found separants for fields of arbitrary characteristic except 5. These are invariants $(B_1, \ldots, B_N)$ of weights $w = (w_1, \ldots, w_N)$ such that

$$f_1 \overset{\mathrm{GL}_2(\bar{k})}{\sim} f_2 \quad \Leftrightarrow \quad (B_i(f_1))_{i=1}^N = (B_i(f_2))_{i=1}^N \text{ in } \mathbb{P}^w.$$

- Our algorithms return these separants (and the known invariants in characteristic 5).
- They can also furnish normalized representatives, for which the isomorphism check reduces to checking an equality.
- Format: `ShiodaInvariants(C : normalize := true)`

Hyperelliptic curves: Reconstruction

Conversely, we want to reconstruct hyperelliptic curves from given Igusa or Shioda invariants I:

That is, we want to find a curve C whose invariants are projectively equivalent to I.

Hyperelliptic curves: Reconstruction

Conversely, we want to reconstruct hyperelliptic curves from given Igusa or Shioda invariants I:

That is, we want to find a curve C whose invariants are projectively equivalent to I.

- Previous work over $\overline{\mathbb{Q}}$ (Clebsch, Mestre, Lercier–Ritzenthaler) described how to obtain a conic Q and a curve H in $\mathbb{P}^2$ of degree $g+1$ such that C is obtained by ramifying over Q in $Q \cap H$. This also works when $\mathrm{char}(k) > 7$.
- Basson's work extends these results to $\mathrm{char}(k) \neq 5$.
- Format: `HyperellipticCurveFromShiodaInvariants(I)`

Hyperelliptic curves: Reconstruction

Using a generalization of the conic variation trick, our reconstruction results in small coefficients, especially over $\mathbb{Q}$.

Hyperelliptic curves: Reconstruction

Using a generalization of the conic variation trick, our reconstruction results in small coefficients, especially over $\mathbb{Q}$.

```
> P<x> := PolynomialRing(Rationals());
> f := x^8 + x^3 + 1;
> f2 := P ! (Evaluate(f, (x+1001)/(3*x+5))*(3*x+5)^8);
> f2;
6805*x^8 + 827242*x^7 + 765112882*x^6 + 306007035874*x^5 +
  723318292142220*x^4 + 56287364680951806*x^3 +
  2816843187239852927 8*x^2 + 8056168289692716824758*x +
  1008028056073190412776751
> I := ShiodaInvariants(f2);
> HyperellipticCurveFromShiodaInvariants(I);
Hyperelliptic Curve defined by y^2 = x^8 + x^3 + 1 over Rational Field
Symmetric group acting on a set of cardinality 2

Order = 2
```

Plane quartic curves: Invariants

Studying moduli of plane quartic curves comes down to studying the space

$$S(k) = \left(\bigoplus_{n \geq 0} \mathrm{Sym}^n(\mathrm{Sym}^4(k^3)) \right)^{\mathrm{SL}_3(k)}.$$

Plane quartic curves: Invariants

Studying moduli of plane quartic curves comes down to studying the space

$$S(k) = \left(\bigoplus_{n \geq 0} \mathrm{Sym}^n(\mathrm{Sym}^4(k^3)) \right)^{\mathrm{SL}_3(k)}.$$

- This time, we get 13 Dixmier–Ohno invariants $I_3, \ldots, I_{27}$ for $k = \mathbb{C}$.
- The discriminant $2^{-40} I_{27}$ is integral in the coefficients. We sped up its computation using work of Laurent Busé.
- If $\mathrm{char}(k) \geq 7$, the Dixmier–Ohno invariants still generate an ideal whose radical contains the irrelevant ideal of $S(k)$ (Lercier–Liu–Lorenzo García–Ritzenthaler, 2018).
- Format: `DixmierOhnoInvariants(C : normalize := true)`

Plane quartic curves: Reconstruction

Work by Lercier–Ritzenthaler–S makes it possible to reconstruct a smooth plane quartic from given Dixmier–Ohno invariants I.

- For this reconstruction, we need that $I_{12} \neq 0$ or that $|\operatorname{Aut}(C)| > 2$. In the latter case, the reconstruction can give rise to problems in characteristic up to 41762629; in the former, it suffices that the characteristic not be ≤ 13 or 79.
- The reconstruction may take place over a quadratic extension if $|\operatorname{Aut}(C)| = 2$; in practice, this does not seem to happen too often.
- The coefficients of our ternary quartic reconstruction are typically small over $\mathbb{Q}$ (combine variation of conics with minimization algorithms by Elsenhans).

Plane quartic curves: Reconstruction

```
> P<x,y,z> := PolynomialRing(GF(31), 3);
> PP := ProjectiveSpace(P);
> f1 := x^4 + 3*y^4 + 5*z^4 + x^2*y*z + x*y*z^2 + x^2*y^2;
> C1 := Curve(PP, f1);
> I := DixmierOhnoInvariants(f1);
> C2 := Curve(PP, TernaryQuarticFromDixmierOhnoInvariants(I));
> IsIsomorphicPlaneQuartics(C1, C2);
true [
 [ 1 24 8]
 [ 8 27 20]
 [13 20 19]
]
```

TODO

Some open problems:

- Determine the structure of the (reduced) automorphism group efficiently.
- Determine generators for the rings of invariants in small characteristic.
- Make reconstruction of smooth plane quartics work in all cases.