Fast computation of isomorphisms of hyperelliptic curves and explicit descent

Reynald Lercier, Christophe Ritzenthaler and Jeroen Sijsling

IRMAR (Rennes), IML (Marseille), IRMAR (Rennes)

ANTS, San Diego
July 11, 2012

Motivation in genus 1

Let K be an algebraically closed field of characteristic $p \neq 2$.

- Elliptic curves $(p \neq 3)$ $E/K \ : y^2 = x^3 + a\,x + b$ are classified up to isomorphism by

$$j(E) = 1728\,\frac{4a^3}{4\,a^3 + 27\,b^2}\,.$$

- Conversely, for any $j \in K \setminus \{0, 1728\}$, we can reconstruct a curve E s.t. $j(E) = j$, for instance

$$E/K : y^2 = x^3 - \frac{27\,j}{j - 1728}\,x + \frac{54\,j}{j - 1728}\,.$$

General genus

- Similarly, we would like to do the same for hyperelliptic curves of genus $g \geq 2$, *i.e.* $C/K : y^2 = f(x)$ with $\deg(f) = 2g + 2$ and simple roots.

$$\{\text{Hyperelliptic curves of genus } g\}_{/\simeq} \longleftrightarrow \{\text{a `space' of parameters}\}$$

- More precisely, given two such curves represented by the same parameters, we would like to find an explicit isomorphism between them.

Applications

- Determining automorphism groups of curves;
- Galois descent for curves;
- Geometric and arithmetic information on the moduli space;
- Reconstructing curves from invariants;
- Applications to cryptography (CM method).

Isomorphisms

Let $C : y^2 = f(x)$ and $C' : y^2 = f'(x)$ be two hyperelliptic curves of genus g. Every isomorphism from C to C' is of the form

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

for some $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(K)$ and $e \in K^*$.

Isomorphisms

Let $C : y^2 = f(x,z)$ and $C' : y^2 = f'(x,z)$ be two hyperelliptic curves of genus g in weighted projective $(1,1,g+1)$-space. Every isomorphism from C to C' is of the form

$$(x,z,y) \mapsto (ax+bz, cx+dz, ey)$$

for some $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(K)$ and $e \in K^*$.

Invariants

Definition

Let $M^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(K)$ act on binary forms $f(x,z)$ of even degree n by $M.f = f(ax+bz, cx+dz)$.

A homogenous polynomial function I on the space of such forms f is an invariant if there exists $\omega \in \mathbb{Z}$ such that for all $M \in \mathrm{GL}_2(K)$,

$$I(M.f) = \det(M)^{\omega} \cdot I(f).$$

Let n, resp. d, be the degree of f, resp. I. If nd is odd then I is zero. Otherwise we have the equality $\omega = nd/2$ for the weight ω of C.

Ex: $f = a_2X^2 + a_1XZ + a_0Z^2$, $I = a_1^2 - 4a_2a_0$ is a degree-2 invariant.

Invariants and isomorphisms

Fact: the algebra of invariants $\mathcal{I}_n$ is finitely generated (Gordan 1868) and for $n \leq 10$ generators are explicitly known.

Theorem (- Mumford 1977)

Let f, f' be binary forms of even degree $n \geq 4$ with simple roots. Let $\{I_i\}$ be a finite set of homogeneous generators of degree d_i for $\mathcal{I}_n$.

Then f and f' are in the same orbit under the action of $\mathrm{GL}_2(K)$ if and only if there exists $\lambda \in K$ such that for all i, $I_i(f) = \lambda^{d_i} \cdot I_i(f')$.

So we can test efficiently whether $C : y^2 = f(x)$ and $C' : y^2 = f'(x)$ are isomorphic by computing a finite set of invariants. But how to obtain these?

Covariant and transvectant

To construct invariants, one needs to embed them in a broader framework.

Definition

A homogeneous polynomial function $C : f \mapsto g$ sending binary forms f of degree n to binary forms g of degree r is a covariant if for all $M \in \mathrm{GL}_2(K)$,

$$C(M.f) = \det(M)^{\omega} \cdot M.C(f).$$

The integer r is called the order of C. If $nd - r$ is odd, C is zero. Otherwise we have the equality $\omega = (nd - r)/2$ for the weight ω of C.

Ex: The identity map is a covariant of order n, degree 1 and weight 0.

We will identify C with $C(f)$ for the tautological form $f \in F(a_0, \ldots, a_n)[x, z]$. Here F is the prime field of K.

On the algebra $\mathcal{C}_n$ of covariants, there are bilinear differential operators, called *h*-th transvectant

$$\Big(\underbrace{C_1}_{\substack{\text{degree } d_1 \\ \text{order } r_1}} , \underbrace{C_2}_{\substack{\text{degree } d_2 \\ \text{order } r_2}} \Big) \mapsto \underbrace{(C_1, C_2)_h}_{\substack{\text{degree } d_1 + d_2 \\ \text{order } r_1 + r_2 - 2h}}$$

Fact (Gordan 1868): starting from the covariant f and applying a finite number of h-th transvectants, one can get a set of generators for $\mathcal{I}_n$ (and for $\mathcal{C}_n$).

Genus 1

Let

$$f = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

There is one covariant of degree 2 and order 4

$$(f,f)_2 = (1/3a_2a_4 - 1/8a_3^2)x^4 + (a_1a_4 - 1/6a_2a_3)x^3 + (2a_0a_4 + 1/4a_1a_3 - 1/6a_2^2)x^2 + (a_0a_3 - 1/6a_1a_2)x + 1/3a_0a_2 - 1/8a_1^2.$$

The algebra of invariants $\mathcal{I}_4$ is generated by

$$I = (f,f)_4 = 2a_0a_4 - 1/2a_1a_3 + 1/6a_2^2$$

and by

$$J = (f,(f,f)_2)_4 = a_0a_2a_4 - 3/8a_0a_3^2 - 3/8a_1^2a_4 + 1/8a_1a_2a_3 - 1/36a_2^3.$$

Rem: The j-invariant is equal to $1728I^3/(I^3 - 6J^2)$.

Computing isomorphisms

Proposition

Let $C_i : y^2 = f_i(x)$ be hyperelliptic curves of genus g. Let c_i be covariants of f_i with non-zero discriminant and $X_i : y^2 = c_i(x)$ the associated hyperelliptic curves. Then, up to the hyperelliptic involution, $\mathcal{I}som(C_1, C_2) \subset \mathcal{I}som(X_1, X_2)$.

Hence, one can recursively reduce the computation to lower genera and/or use a new basic method to deal with this easier case.

Generically, one can use the quartic covariant $(f, f)_{n-2}$. This yields fast algorithms:

Field	Method	Genus g										
		1	2	4	8	16	32	64	128	256	512	1024
$\mathbb{F}_{10007}$	`IsGL2Equivalent`	0	0	0	0	0.1	0.2	0.9	6.5	39	242	1560
	`IsGL2EquivFast`	0	0	0	0	0	0	0.1	0.6	3.7	25	165
	`IsGL2EquivCovariant`	0	0	0	0	0	0	0	0	0.1	0.5	2.5
$\mathbb{Q}$	`IsGL2Equivalent`	0	0	0.4	15	1150	-	-	-	-	-	-
	`IsGL2EquivFast`	0	0	0	0	0.1	0.2	0.6	3	30	382	5850
	`IsGL2EquivCovariant`	0	0	0	0	0	0	0	0.2	0.6	3.4	7

Galois descent

So far, we worked over an algebraically closed field, but what happens if now $k \subset \overline{k} = K$ is any field (of characteristic 0 or a finite field) ?

Definition

Let C/K be a curve of genus $g \geq 2$.

A field k is a field of definition for C if there exists a curve $\mathcal{C}/k$ (called a model of C) which is K-isomorphic to C.

The intersection $\mathbf{M}_C$ of all the fields of definition is called the field of moduli of C.

One has also $\mathbf{M}_C = K^H$ where $H = \{\sigma \in \mathrm{Aut}(K),\ C \simeq {}^{\sigma}C\}$ and it is the residue field of the point $[C]$ in the coarse moduli space M_g.

$\mathbf{M}_C$ is a field of definition when

- C has no automorphisms;
- K is the algebraic closure of a finite field.

Galois descent and covariants

Theorem

Let $C : y^2 = f(x)$, let c be a covariant of f with non-zero discriminant and let $X : y^2 = c(x)$ be the associated curve. Suppose that X is (hyperelliptically) defined over its field of moduli.
Then C is (hyperelliptically) defined over an extension of its field of moduli of degree at most $[\mathrm{Aut}_K(X) : \# \mathrm{Aut}_K(C)]$.

The proof yields the following explicit descent method:

- Calculate a non-degenerate covariant c of f;
- Descend the covariant curve X (automatic in genus 1);
- Compute the descent morphism by our earlier algorithms;
- Apply the descent morphism to C.

Example for $g = 3$ with C_2^3

$$(j_2 : j_3 : \dots : j_{10}) = \left(0 : 0 : -\frac{25}{98} : -\frac{25}{98} : -\frac{225}{2744} : -\frac{25}{1372} : -\frac{225}{134456} : \frac{1125}{76832} : \frac{15125}{3764768}\right).$$

This gives rise to the curve $C : y^2 = f(x)$ with $\mathrm{Aut}_K(C) \simeq C_2^3$ and

$$f(x) = (-32\,\alpha^2 + 420\,\alpha - 2275)/160\,x^8 + (-12\,\alpha^2 + 140\,\alpha - 700)/25\,x^6 + \alpha\,x^4 + x^2 + (16\,\alpha^2 + 280\,\alpha - 2275)/12250$$

over $\mathbb{Q}(\alpha)$, where $\alpha^3 - 35/2\,\alpha^2 + 1925/16\,\alpha - 18375/64 = 0$.

Take the covariant curve $X : y^2 = c(x)$ with $\mathrm{Aut}_K(X) \simeq C_2^3$ where

$$c = (f,f)_6 = (-16\,\alpha^2 + 180\,\alpha - 875)/280\,x^4 + (24\,\alpha^2 - 630\,\alpha + 3150)/1225\,x^2 + (4\,\alpha + 35)/490.$$

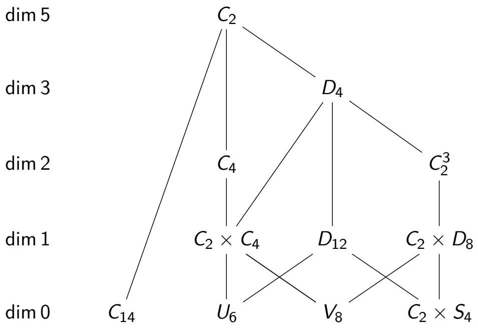
$I = -75/49$, $J = -2025/343$ so $X \simeq_K \mathfrak{X} : y^2 = x^3 + 25/9\,x + 25/9$.

We compute $\phi : X \to \mathfrak{X}$ and apply it to C:

$$\phi(C) : y^2 = x^8 + 160\,x^7 - 560\,x^6 - 2800\,x^5 + 64750\,x^4 - 91000\,x^3 + 3010000\,x^2 - 2225000\,x - 9696875\,.$$

Reconstruction in genus 3

$g = 3$ (char $K \neq 2, 3, 5, 7$)



- Reconstruction is possible for the C_2 and C_4 cases by Mestre's method;
- Gröbner basis methods give results for the strata of dimension ≤ 1;
- For C_2^3, these methods yield an extension, but we can descend as before;
- For D_4, a descent to the field of moduli does not always exist.

The D_4 case and beyond genus 3

The *reduced automorphism group* $\overline{\mathrm{Aut}}(C)$ of C is $\mathrm{Aut}(C)$ modulo the hyperelliptic involution.

Theorem (Huggins 2007)

Let C/K be a hyperelliptic curve whose reduced automorphism group is not cyclic. Then its field of moduli is a field of definition.

For general g and $|\overline{\mathrm{Aut}}(C)|$, work in progress has made explicit the obstruction for C to be defined over its field of moduli. It is determined by the splitting of a certain quaternion algebra determined by the invariants of C.

Conclusion

- For $g = 3$, extend our results to small characteristics $2 \leq p \leq 7$ (Lercier - Basson).
- For hyperelliptic curves, prove that if $p > 2g + 1$, Gordan's method generates all invariants.
- For hyperelliptic curves, develop our functions in Sage (work in progress by Rovetta).
- For hyperelliptic curves, develop algorithms to compute twists over finite fields (work in progress by Rovetta).
- Generalize the computations of isomorphisms to ternary forms (work in progress for plane quartics; *cf.* earlier results by Van Rijnswou).