Invariants and hyperelliptic curves: geometric, arithmetic and algorithmic aspects

R. Lercier, C. Ritzenthaler

IML - CNRS (Marseille)

Luminy, October 2011

The genus 1 case

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

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

- 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.

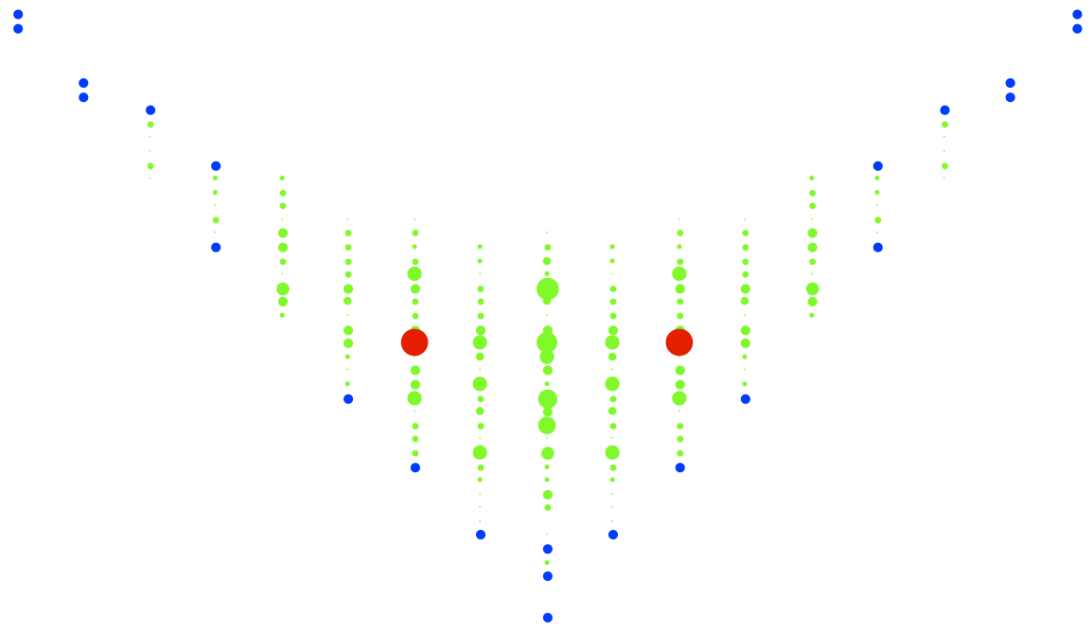
$$\{\text{Hyperelliptic curves of genus } g\}_{/\simeq} \longleftrightarrow \{\text{a 'space' of parameters}\}$$

Concretely for $g = 3$...

```
> _<x> := PolynomialRing(GF(11));
> H1 := HyperellipticCurve(7*x^8 + 5*x^6 + 5*x^4 + 3*x^2 + x + 9);

> ShiodaInvariants(H1);
[ 8, 2, 4, 10, 2, 7, 8, 9, 3 ]

> H2, G := HyperellipticCurveFromShiodaInvariants($1); H2;
Hyperelliptic Curve defined by
  y^2 = x^8 + x^7 + x^6 + 4*x^5 + x^4 + x^2 + 5*x + 8 over GF(11)

> IsIsomorphic(H1, H2);
true
> IdentifyGroup(G);
<8, 5>
```

Why do we want do be able to do this ?

- check if two curves are isomorphic;
- recognize quickly the group of automorphisms;
- Information about the moduli space;
- arithmetic properties: what is the smallest field over which I can define the curve ?
- enumeration of curves over finite fields for experiments.



Distribution of of genus 2 curves over $\mathbb{F}_7$ among isogeny classes

Isomorphisms

Proposition

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* $e \in K^*$. *The couple* (M, e) *is unique up to* $(\lambda \cdot M, \lambda^{g+1} \cdot e)$.

Invariants

Definition

Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(K)$ 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 $M \in \mathrm{GL}_2(K)$,

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

If I has degree d then its weight $\omega = nd/2$.

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

Necessary results on invariant algebras

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, $I_i(f) = \lambda^{d_i} \cdot I_i(f')$.

$\Rightarrow$ test efficiently if $C : y^2 = f(x)$ and $C' : y^2 = f'(x)$ are isomorphic by computing a finite set of invariants.

Covariant and transvectant

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

Definition

Let M acts on a vector $(x, z) \in K^2$ by $M.(x, z) = M^{-1} \begin{pmatrix} x \\ z \end{pmatrix}$.

A bihomogeneous polynomial function $C(f, (x, z))$ is a covariant C for binary forms $f(X, Z)$ of even degree n if there exists $\omega \in \mathbb{Z}$ such that for all $M \in \mathrm{GL}_2(K)$,

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

The degree r of C in (x, z) is called the order. One has $\omega = (nd - r)/2$.

Ex: $C : (\sum a_i X^i Z^{n-i}, (x, z)) \mapsto \sum a_i x^i z^{n-i}$ is a covariant of order n, degree 1 and weight 0.

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 $\mathcal{C}_n$).

Shioda invariants for $\mathcal{I}_8$

(Shioda 1967) defines the invariants J_i's as

$$J_2 = (f,f)_8,\ J_3 = (f,\mathfrak{g})_8,\ J_4 = (\mathfrak{k},\mathfrak{k})_4,\ J_5 = (\mathfrak{m},\mathfrak{k})_4,\ J_6 = (\mathfrak{k},\mathfrak{h})_4,$$
$$J_7 = (\mathfrak{m},\mathfrak{h})_4, J_8 = (\mathfrak{p},\mathfrak{h})_4,\ J_9 = (\mathfrak{n},\mathfrak{h})_4,\ J_{10} = (\mathfrak{q},\mathfrak{h})_4$$

where

$$\mathfrak{g} = (f,f)_4,\ \mathfrak{k} = (f,f)_6,\ \mathfrak{h} = (\mathfrak{k},\mathfrak{k})_2,\ \mathfrak{m} = (f,\mathfrak{k})_4,\ \mathfrak{n} = (f,\mathfrak{h})_4,\ \mathfrak{p} = (\mathfrak{g},\mathfrak{k})_4,\ \mathfrak{q} = (\mathfrak{g},\mathfrak{h})_4\,.$$

Rem: These formulas are valid over fields of char. p with $p = 0$ or $p > 7$.

Theorem (Shioda 1967)

$\mathcal{I}_8$ is generated by the 9 invariants J_2, J_3, ..., J_{10} of deg. 2, 3, ..., 10. $J_2, \ldots, J_7$ are algebraically independent and there exist 5 generating relations, $\mathfrak{R}_i(J)$ between the J_is.

According to the syzygy theorem of Hilbert, $\mathcal{I}_8$ fits into a finite exact sequence of $\mathbb{C}[X] := \mathbb{C}[X_2, \ldots, X_{10}]$-module.

$$0 \to \mathbb{C}[X]\mathfrak{F} \to \sum_{i=1}^{5} \mathbb{C}[X]\mathfrak{T}_i \to \sum_{i=1}^{5} \mathbb{C}[X]\mathfrak{R}_i \to \mathbb{C}[X] \to \mathcal{I}_8 \to 0\,.$$

Example

Ex. : $\mathrm{Disc}(f)$ is an invariant of deg. 14. We find

$$\begin{aligned}\mathrm{Disc}(f) = {} & 29008561427982581760\, J_{10}\, J_4 + 18346188403113984000\, J_{10}\, J_2^2 - 21756421070986936320\, J_9\, J_5 \\ & - 7554312871870464000\, J_9\, J_3\, J_2 - 3021725148748185600\, J_8\, J_6 + 31803657190574653440\, J_8\, J_4\, J_2 \\ & + 2549580594256281600\, J_8\, J_3^2 + 2345327219866337280\, J_8\, J_2^3 - 106232524760678400\, J_7^2 \\ & - 8849169312564510720\, J_7\, J_5\, J_2 - 5139293475644375040\, J_7\, J_4\, J_3 - 1292776756346880000\, J_7\, J_3\, J_2^2 \\ & + 4879526536497070080\, J_6^2\, J_2 + 4582949808934748160\, J_6\, J_5\, J_3 + 2751208802098348032\, J_6\, J_4^2 \\ & + 1267160326927810560\, J_6\, J_4\, J_2^2 - 1143872189796188160\, J_6\, J_3^2\, J_2 - 93857730923593728\, J_6\, J_2^4 \\ & - 895451656628551680\, J_5^2\, J_2^2 + 351157512403353600\, J_5\, J_4\, J_3\, J_2 + 212465049521356800\, J_5\, J_3^3 \\ & - 66189456176578560\, J_5\, J_3\, J_2^3 + 968390964336918528\, J_4^3\, J_2 + 169419330714009600\, J_4^2\, J_3^2 \\ & + 313290675380551680\, J_4^2\, J_3\, J_2^2 + 33474799101542400\, J_4\, J_3^2\, J_2^2 - 16397790463918080\, J_4\, J_2^5 \\ & + 31476303632793600\, J_3^4\, J_2 + 10245839137013760\, J_3^2\, J_2^4 + 369994358063104\, J_2^7\ .\end{aligned}$$

Reconstruction

- Starting from a 'list' $(j_1 : j_2 : \ldots)$ of values of $J_i(f)$ in K, we aim at recovering a hyperelliptic curve C/K, isomorphic to $y^2 = f(x)$.

- In general, inverting the polynomial system giving the invariants in terms of a generic polynomial $f = \sum_i a_i x^i$ is quickly impossible.

$$J_2 = 2\,a_0\,a_8 - \frac{1}{4}\,a_1\,a_7 + \frac{1}{14}\,a_2\,a_6 - \frac{1}{28}\,a_3\,a_5 + \frac{1}{70}\,{a_4}^2,$$

$$J_3 = \frac{3}{35}\,a_0\,a_4\,a_8 - \frac{3}{56}\,a_0\,a_5\,a_7 + \frac{9}{392}\,a_0\,{a_6}^2 - \frac{3}{56}\,a_1\,a_3\,a_8 + \frac{9}{560}\,a_1\,a_4\,a_7 - \frac{3}{784}\,a_1\,a_5\,a_6 + \frac{9}{392}\,{a_2}^2 a_8$$
$$- \frac{3}{784}\,a_2\,a_3\,a_7 - \frac{33}{13720}\,a_2\,a_4\,a_6 + \frac{9}{5488}\,a_2\,{a_5}^2 + \frac{9}{5488}\,{a_3}^2 a_6 - \frac{27}{27440}\,a_3\,a_4\,a_5 + \frac{9}{34300}\,{a_4}^3,$$

$$J_4 = \cdots$$

- However, (Mestre 1991) suggested a general strategy based on nice formulae due to (Clebsch 1872).

Generic reconstruction

1. Choose 3 covariants q_1, q_2, q_3 of order 2;

2. Construct from them a conic $\mathcal{Q} : \sum A_{ij} \cdot x_i x_j = 0$ and a plane degree $g+1$ curve $\mathcal{H} : \sum h_I \cdot x_I = 0$ satisfying

   - A_{ij} and h_I are invariants;
   - The point $(x_1^* : x_2^* : x_3^*) = ((q_2, q_3)_1 : (q_3, q_1)_1 : (q_1, q_2)_1)$ is solution of

$$\begin{cases} \sum A_{ij} \cdot x_i^* x_j^* = 0, \\ \sum h_I \cdot x_I^* - R(q_1, q_2, q_3)^{n/2} \cdot f(x, z) = 0, \end{cases}$$

   where $R(q_1, q_2, q_3)$ is zero iff the conic $\mathcal{Q}$ is singular.

3. After parametrization of $\mathcal{Q}$, the intersection points of $\mathcal{Q}$ and $\mathcal{H}$ are $\mathrm{GL}_2(K)$-equivalent to the zeros of f.

Example for $g = 3$

Choose $q_1 = C_{5,2}$, $q_2 = C_{6,2}$ and $q_3 = C_{7,2}$ (one among 364 choices).

$R(q_1, q_2, q_3)$ is the determinant of the q_i's in the basis x^2, xz, z^2.

Up to a constant,

$$
\begin{aligned}
R(q_1, q_2, q_3) = &-4937630140800 {J_9}^2 + 6172588800000 J_8 J_{10} + 1016336160000 {J_6}^3 - 1646487542700 J_5 J_6 J_7 + 475344450 {J_5}^2 J_8 \\
&- 13778100 J_4 {J_7}^2 + 6154254741600 J_4 J_6 J_8 + 2469123699840 J_4 J_5 J_9 - 3175414824960 {J_4}^2 J_{10} \\
&- 1028718873000 J_3 J_7 J_8 - 1555231104000 J_3 J_6 J_9 + 514676332800 J_3 J_5 J_{10} - 579162433500 J_2 {J_8}^2 \\
&+ 231655788000 J_2 J_7 J_9 + 47632860 {J_4}^2 {J_5}^2 - 201602675520 {J_4}^3 J_6 - 264617457390 J_3 J_4 J_5 J_6 \\
&+ 529262244990 J_3 {J_4}^2 J_7 + 4618063800 {J_3}^2 {J_6}^2 - 35210700 {J_3}^2 J_5 J_7 - 228766979700 {J_3}^2 J_4 J_8 \\
&+ 38124172800 {J_3}^3 J_9 + 77149935135 J_2 {J_5}^2 J_6 - 40603006080 J_2 J_4 {J_6}^2 - 115812049185 J_2 J_4 J_5 J_7 \\
&- 330859026540 J_2 {J_4}^2 J_8 + 145802916000 J_2 J_3 J_6 J_7 - 15715198800 J_2 J_3 J_4 J_9 + 42877447200 J_2 {J_3}^2 J_{10} \\
&+ 53596043550 {J_2}^2 {J_7}^2 - 145802916000 {J_2}^2 J_6 J_8 - 53606606760 {J_2}^2 J_5 J_9 + 137217628800 {J_2}^2 J_4 J_{10} \\
&- 36737464140 {J_3}^2 {J_4}^3 - 7824600 {J_3}^3 J_4 J_5 + 11300902200 {J_3}^4 J_6 - 47249726760 J_2 {J_4}^4 \\
&- 12161979900 J_2 J_3 {J_4}^2 J_5 + 33446455740 J_2 {J_3}^2 J_4 J_6 + 1760535 {J_2}^2 J_4 {J_5}^2 + 25514097660 {J_2}^2 {J_4}^2 J_6 \\
&- 153935460 {J_2}^3 {J_6}^2 + 1173690 {J_2}^3 J_5 J_7 + 7625565990 {J_2}^3 J_4 J_8 - 1270805760 {J_2}^3 J_3 J_9 - 1429248240 {J_2}^4 J_{10} \\
&+ 289800 J_2 {J_3}^4 J_4 + 900887400 {J_2}^2 {J_3}^2 {J_4}^2 + 2575261188 {J_2}^3 {J_4}^3 + 260820 {J_2}^3 J_3 J_4 J_5 - 753393480 {J_2}^3 {J_3}^2 J_6 \\
&- 1114881858 {J_2}^4 J_4 J_6 - 19320 {J_2}^4 {J_3}^2 J_4 - 30029580 {J_2}^5 {J_4}^2 + 12556558 {J_2}^6 J_6 + 322 {J_2}^7 J_4 \,.
\end{aligned}
$$

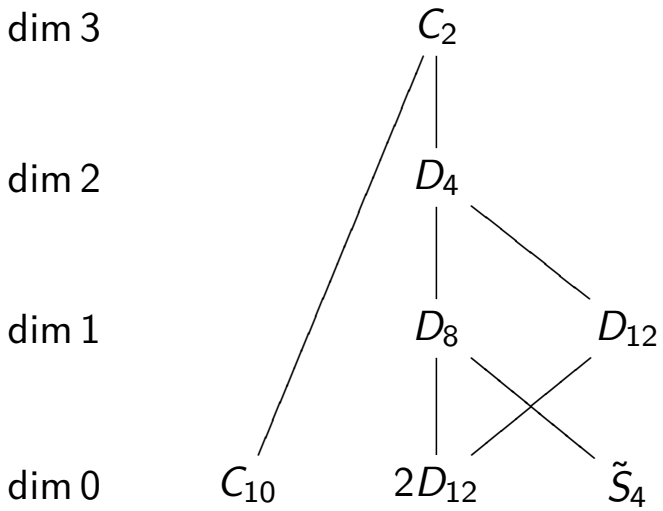
Example (cont.)

$$\begin{aligned}\mathcal{Q}\ : 0 = {} & (9217732608000 J_{10} - 1422489600 {J_2}^3 J_4 + 1814283878400 J_4 J_6 - 384072192000 J_3 J_7 + 42674688000 {J_3}^2 J_4 \\ & - 1152216576000 {J_5}^2 + 212154163200 J_2 {J_4}^2 + 384072192000 J_2 J_8)\ {x_1^*}^2 \\ & + (-80015040000 {J_3}^2 J_5 + 2667168000 {J_2}^3 J_5 - 12002256000 {J_2}^2 J_7 + 288054144000 J_2 J_9 + 216040608000 J_4 J_7 \\ & - 102019176000 J_2 J_4 J_5 + 138883248000 J_3 {J_4}^2 - 48009024000 J_5 J_6 + 360067680000 J_3 J_8)\ x_1^* x_2^* \\ & + (-12040358400 {J_2}^2 J_8 - 902039040 {J_2}^3 J_6 - 24768737280 {J_4}^3 + 27061171200 {J_3}^2 J_6 + 18627840 {J_2}^4 J_4 \\ & - 424308326400 J_2 J_{10} - 5482391040 {J_2}^2 {J_4}^2 - 43481733120 J_2 J_4 J_6 + 216726451200 J_5 J_7 + 12040358400 J_2 J_3 J_7 \\ & - 762657638400 J_4 J_8 + 36121075200 J_2 {J_5}^2 + 135339724800 J_3 J_9 - 162570240000 {J_6}^2 - 10516262400 J_3 J_4 J_5 \\ & - 558835200 J_2 {J_3}^2 J_4)\ x_1^* x_3^* + (135025380000 J_3 J_9 + 55566000 {J_2}^3 J_6 - 15788682000 J_2 J_4 J_6 + 2813028750 {J_2}^2 J_8 \\ & - 2813028750 J_2 J_3 J_7 + 149333625 {J_2}^4 J_4 + 8439086250 J_3 J_4 J_5 - 151903552500 J_4 J_8 - 2509400250 {J_2}^2 {J_4}^2 \\ & + 75951776250 J_5 J_7 - 1666980000 {J_3}^2 J_6 - 4480008750 J_2 {J_3}^2 J_4 + 92610000 {J_2}^3 {J_3}^2 - 1543500 {J_2}^6 \\ & - 1389150000 {J_3}^4 - 2893401000 {J_4}^3 - 50009400000 {J_6}^2 - 67512690000 J_2 J_{10})\ {x_2^*}^2 \\ & + (1434793500 {J_2}^2 J_4 J_5 - 1629217800 J_2 J_3 {J_4}^2 + 6460738200 J_2 J_5 J_6 + 365148000 {J_3}^3 J_4 - 41806800 {J_2}^4 J_5 \\ & - 12748654800 J_3 J_4 J_6 + 1254204000 J_2 {J_3}^2 J_5 + 914457600 J_2 J_4 J_7 - 12171600 {J_2}^3 J_3 J_4 - 172254600 {J_2}^3 J_7 \\ & - 2400451200 {J_2}^2 J_9 - 714420000 J_6 J_7 - 5643918000 J_2 J_3 J_8 - 4445733600 {J_4}^2 J_5 + 14402707200 J_4 J_9 \\ & + 10811556000 {J_3}^2 J_7 - 63440496000 J_3 J_{10} - 44365482000 J_5 J_8)\ x_2^* x_3^* \\ & + (94363920 {J_2}^3 J_8 + 2592705024 {J_4}^2 J_6 - 32568480 {J_3}^2 {J_4}^2 + 57512 {J_2}^5 J_4 - 283091760 {J_2}^2 {J_5}^2 + 4386130560 {J_2}^2 J_{10} \\ & - 1905120000 J_6 J_8 - 40824000 {J_7}^2 + 34895088 {J_2}^3 {J_4}^2 + 1886976000 J_2 {J_6}^2 - 10150479360 J_5 J_9 \\ & - 109801152 {J_2}^2 J_4 J_6 + 23227223040 J_4 J_{10} + 21819168 {J_2}^4 J_6 + 3110425920 J_3 J_5 J_6 + 15630965280 J_2 J_4 J_8 \\ & + 164838240 J_2 J_3 J_4 J_5 + 635065920 J_2 {J_4}^3 - 3676609440 J_3 J_4 J_7 - 1725360 {J_2}^2 {J_3}^2 J_4 - 3397101120 J_2 J_5 J_7 \\ & - 2121396480 J_2 J_3 J_9 - 94363920 {J_2}^2 J_3 J_7 - 654575040 J_2 {J_3}^2 J_6)\ {x_3^*}^2 .\end{aligned}$$

$$\begin{aligned}\mathcal{H}\ : 0 = {} & (20832487200\ {J_7}^3 - 98761420800\ J_6\ J_7\ J_8 - 14814213120\ {J_6}^2 J_9 + 140619288600\ J_5\ {J_8}^2 + 21526903440\ J_5\ J_7\ J_9 \\ & + 192584770560\ J_4\ J_8\ J_9 - 29628426240\ J_3\ {J_9}^2 + 6351593875200000\ J_2\ J_9\ J_{10} - 231472080\ {J_5}^3 J_6 \\ & + 17310682368\ J_4\ J_5\ {J_6}^2 - 24651776520\ J_4\ {J_5}^2 J_7 + \cdots + 653457959280\ {J_2}^5 J_5\ J_6 - 653460684660\ {J_2}^5 J_4\ J_7 \\ & + 108909756900\ {J_2}^6 J_9 + 47040\ {J_2}^4 {J_3}^3 J_4 + 56723695560\ {J_2}^5 J_3\ {J_4}^2 + 141120\ {J_2}^5 {J_3}^2 J_5 + 222264\ {J_2}^6 J_4\ J_5 \\ & + 117600\ {J_2}^6 J_3\ J_6 + 7056\ {J_2}^7 J_7 - 784\ {J_2}^7 J_3\ J_4 - 2352\ {J_2}^8 J_5)\ {x_1^*}^4 + \cdots\end{aligned}$$

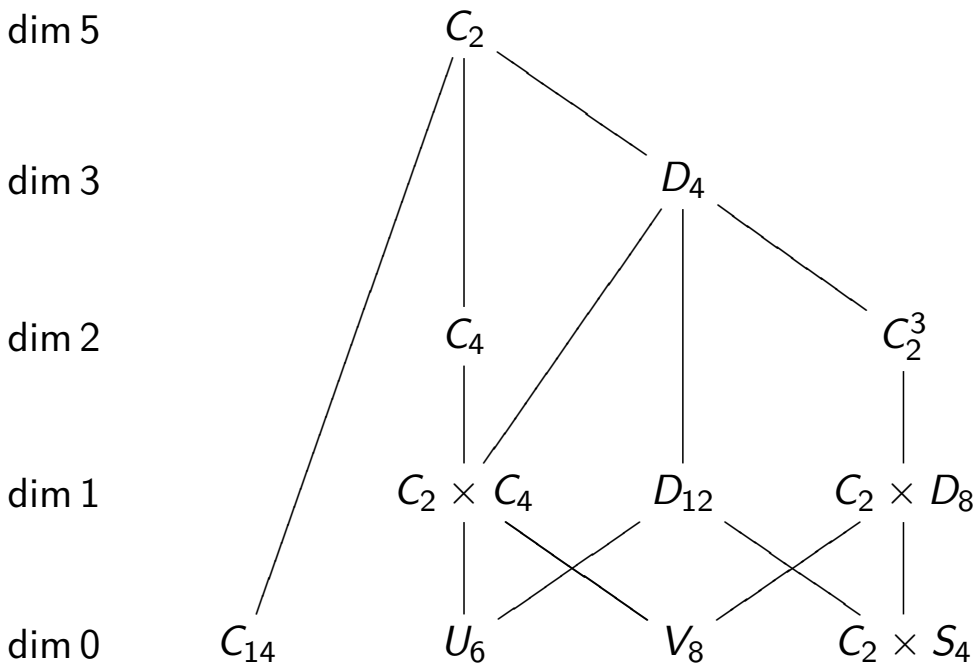
Comparison $g = 2$ and $g = 3$

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



- $\exists\ q_i$ such that $R(q_1, q_2, q_3) \neq 0$ if and only if $\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z}$ (Bolza 1887);
- $\exists\ q'_i$ such that if $\mathrm{Aut}(C) \simeq D_4$, (Cardona and Quer 2005) then $R(q'_1, q'_2, q'_3) \neq 0$;
- For bigger automorphism groups, explicit parametrizations were known.

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



- If $D_4 \subset \mathrm{Aut}(C)$, all possible $R(q_1, q_2, q_3) = 0$;
- For C_4, we found 5 R's among which at least one is non-zero;
- We give explicit parametrizations for dimension 1 cases;
- Conjecture: at least one of the 364 possible R's is non-zero if $\mathrm{Aut}(C) \simeq C_2$;
- Under Conjecture, explicit (parametric when dim ≤ 2) equations and reconstructions for all strata.

Field of moduli and field of definition

So far, we worked over an algebraically closed field, but what happens if now $k \subset \bar{k} = K$ 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

- when C has no automorphism (Dèbes, Ensalem 1999);
- when K is the algebraic closure of a finite field;

Hyperelliptic curves

Definition

A curve C/k is said hyperelliptic if there exists a degree-2 cover to a non singular plane conic Q.

It is of the form $y^2 = f(x)$ when $Q(k) \neq \emptyset$. This leads to the more precise issue.

Definition

We say that C/K can be hyperelliptically defined over k if there exists a model $\mathcal{C}/k$ of C given by $\mathcal{C} : y^2 = f(x)$.

'To be defined' and 'to be hyperelliptically defined' over k are equivalent problems when g is even (Mestre 1991).

Hyperelliptic curves with $\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z}$

Proposition

When g is odd, $\mathbf{M}_C$ is a field of definition.

(Quotients of) Invariants can be seen as functions on the moduli space. In particular if $C : y^2 = f(x)$ then the invariants $I(f)$ of f are naturally defined (as a weighted projective point) over $\mathbf{M}_C$.

Reconstruction of a hyperelliptic model over $\mathbf{M}_C$:

1. Compute a non-singular $\mathcal{Q}$ and $\mathcal{H}$ with coefficients in $\mathbf{M}_C$;
2. If $\mathcal{Q}(\mathbf{M}_C) \neq \emptyset$ then choose a parametrization over $\mathbf{M}_C$ and construct a model $y^2 = \tilde{f}(x)$ of C over $\mathbf{M}_C$;
3. if not, then one can prove that C cannot be hyperelliptically defined over $\mathbf{M}_C$.

Hyperelliptic curves with $\mathbb{Z}/2\mathbb{Z} \subsetneq \mathrm{Aut}(C)$

Theorem (Huggins 2007)

If $\mathrm{Aut}(C)/\langle\iota\rangle$ *is not cyclic then* C *can be hyperelliptically defined over* $\mathbf{M}_C$.

Our work for $g = 3$

- Our parametrizations for the dim ≤ 1 cases were hyperelliptically defined over $\mathbf{M}_C$;
- For C_2^3, we know how to hyperelliptically reconstruct over at most a cubic extension of $\mathbf{M}_C$;
- For D_4, there are couterexamples for $\mathbf{M}_C$ to be a field of definition (Huggins 2007). Our reconstruction is over a degree 8 extension;
- For C_4, we prove using the ramification signature that C can be defined over $\mathbf{M}_C$. Then using Weil cocycle relations, we could hyperelliptically define C over $\mathbf{M}_C$.

Conclusion

Enough to get enumeration over small finite fields:

p	C_2	D_4	C_4	C_2^3	$C_2 \times C_4$	D_{12}	$C_2 \times D_8$	C_{14}	U_6	V_8	$C_2 \times S_4$	Total $= p^5$
11	159729	1092	101	101	8	8	8	1	1	1	1	161051
13	369107	1862	145	145	10	10	10	1	1	1	1	371293
17	1414959	4338	257	257	14	14	14	1	1	1	1	1419857
19	2469257	6140	325	325	16	16	16	1	1	1	1	2476099
23	6424197	11112	485	485	20	20	20	1	1	1	1	6436343

Several open questions:

- Is the condition '$\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z}$' sufficient for the existence of a non-singular conic $\mathcal{Q}$? In any genus ?
- Can we find a hyperelliptic model over $\mathbf{M}_C$ when $\mathrm{Aut}(C) \simeq C_2^3$? A similar question for $g = 5$ showed that the isomorphism to descend the curve can live in a large extension.
- For $g = 3$ can one extend the results to small characteristics ? Can we prove that for $p > 2g + 1$, Gordan's approach works for any g ?