Decomposing Jacobians via Galois Covers

Davide Lombardo, **Elisa Lorenzo García**, Christophe Ritzenthaler, Jeroen Sijsling

Université de Neuchâtel

19-08-2021

Poincaré Reducibility Theorem

Theorem (Poincaré)

Let B be an abelian variety, then there exist unique (up to isogeny) simple abelian varieties A_i and exponents e_i such that:

$$B \sim A_1^{e_1} \times \ldots \times A_r^{e_r}.$$

Poincaré Reducibility Theorem

Theorem (Poincaré)

Let B be an abelian variety, then there exist unique (up to isogeny) simple abelian varieties A_i and exponents e_i such that:

$$B \sim A_1^{e_1} \times \ldots \times A_r^{e_r}.$$

How to explicitly compute this decomposition?

Poincaré Reducibility Theorem

Theorem (Poincaré)

Let B be an abelian variety, then there exist unique (up to isogeny) simple abelian varieties A_i and exponents e_i such that:

$$B \sim A_1^{e_1} \times \ldots \times A_r^{e_r}.$$

How to explicitly compute this decomposition?

Assume $B = J(X)$:

- automorphisms (Kani-Rosen).
- degree d morphisms: $\phi : X \to Y$, then $J(X) \sim J(Y) \times P$

State of the art

- $g(X) = 0, 1$: easy!
- $g(X) = 2$: $d = 2$ Jacobi; $d = 3$ Goursat, Kuhn; $d = 4$ Bolza, Bruin-Doerkesen; $d = 5$ MSV; $d \leq 11$ Kumar.
- unramified double covers ($d = 2$) by Mumford.
- $d = 2$, X hyperelliptic and 2 ramification points: Dalaljan, Levin.
- Galois-theoretic considerations by Donagi: trigonal construction.
- Recillas-Rodriguez: fourfold covers.
- Lang-Ortega: étale cover hyperelliptic curves, triple covers, etc.
- Bruin: $g_X = 5$, $g_Y = 3$, $d = 2$.
- Ritzenthaler-Romagny: $g_X = 3$, $g_Y = 1$, $d = 2$.

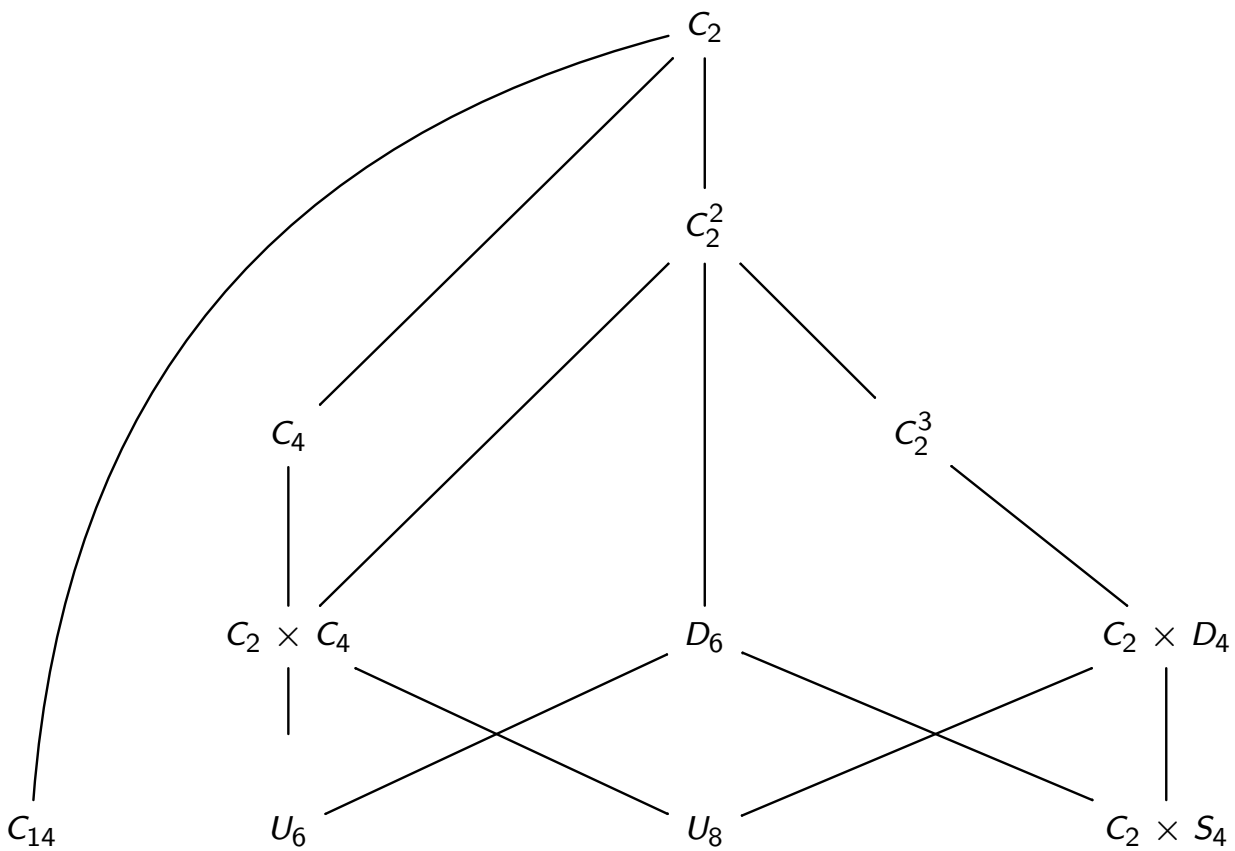
Automorphisms strategy: $g = 3$.

Remark:

If $\phi : X \to Y$ is **Galois** then $\mathrm{Gal}(K(X)/K(Y)) \subseteq \mathrm{Aut}(X)$.

Automorphisms strategy: $g = 3$.

Hyperelliptic genus 3 curves stratification by automorphisms



dim = 5

dim = 3

dim = 2

dim = 1

dim = 0

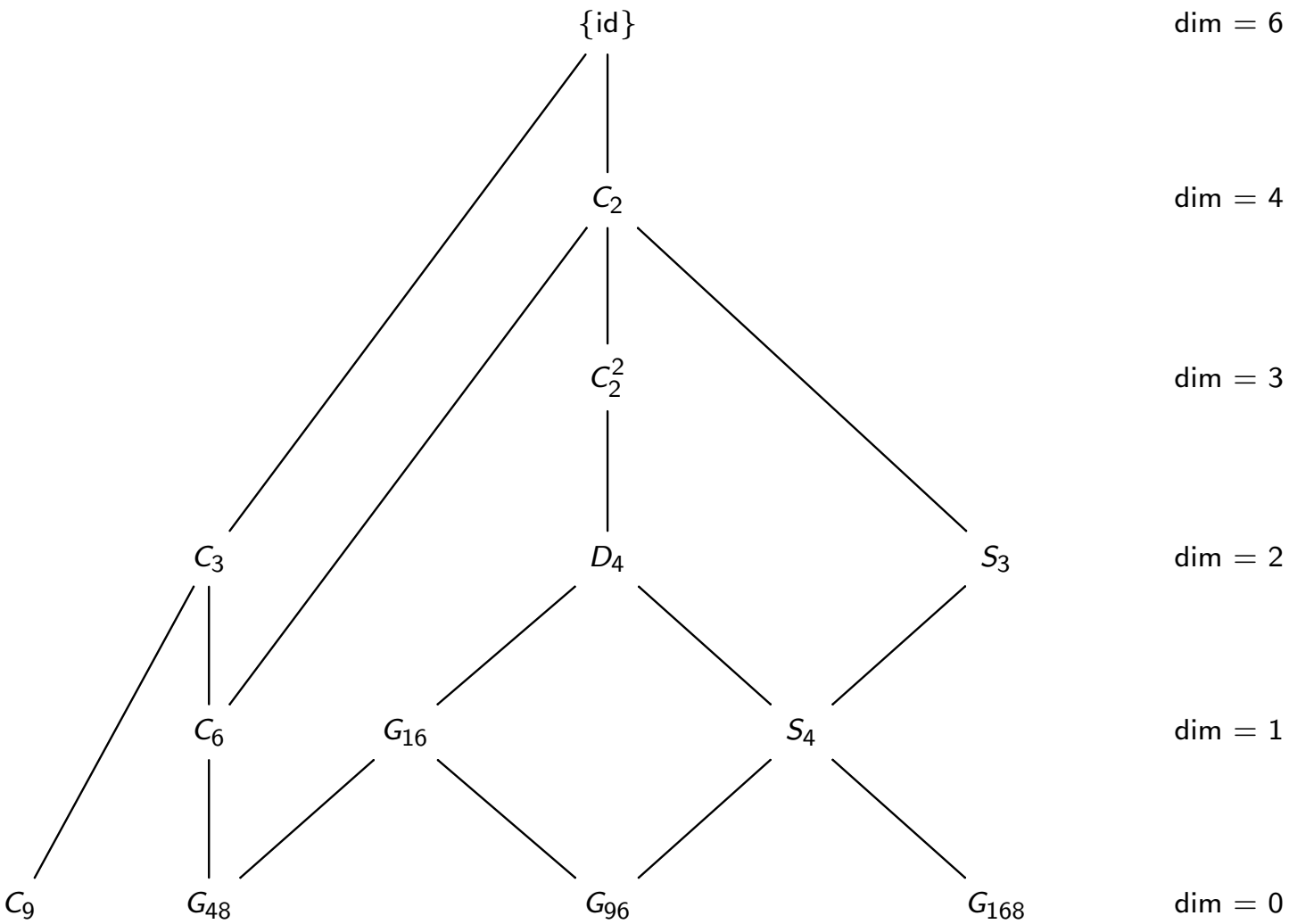
Automorphisms strategy: $g = 3$.

G	$X : y^2 = f(x)$	$\mathrm{J}(X) \sim \prod_{i \in I} \mathrm{J}(C_i)$	Curves C_i
C_2			$\mathrm{J}(X)$ generically simple
C_2^2	$x^8 + ax^6 + bx^4 + cx^2 + 1$	$I = [1, 2]$	$\begin{cases} C_1 : & y^2 = x^4 + ax^3 + bx^2 + cx + 1, \\ C_2 : & y^2 = x(x^4 + ax^3 + bx^2 + cx + 1) \end{cases}$
C_2^3	$x^8 + ax^6 + bx^4 + ax^2 + 1$	$I = [1, 2, 3]$	$\begin{cases} C_1 : & y^2 = x^4 + ax^3 + bx^2 + ax + 1, \\ C_2 : & y^2 = x^4 + (a-4)x^2 - 2a + b + 2 \\ C_3 : & y^2 = x^4 + (a+4)x^2 + 2a + b + 2 \end{cases}$
C_4	$x(x^2 - 1)(x^4 + ax^2 + b)$		$\mathrm{J}(X)$ generically simple with endomorphism algebra $\mathbb{Q}(i)$
$C_2 \times C_4$	$x^8 + ax^6 - ax^2 - 1 = (x^4 - 1)(x^4 + ax^2 + 1)$	$I = [1, 2]$	$\begin{cases} C_1 : & y^2 = (x^2 - 1)(x^2 + ax + 1) \\ C_2 : & y^2 = x(x^2 - 1)(x^2 + ax + 1) \end{cases}$
D_6	$x(x^6 + ax^3 + 1)$	$I = [1, 2, 2]$	$\begin{cases} C_1 : & y^2 = x(x^2 + ax + 1) \\ C_2 : & y^2 = x^3 - 3x + a \end{cases}$
$C_2 \times D_4$	$x^8 + ax^4 + 1$	$I = [1, 2, 2]$	$\begin{cases} C_1 : & y^2 = x^4 + ax^2 + 1 \\ C_2 : & y^2 = x^4 - 4x^2 + (a+2) \end{cases}$
C_{14}	$x^7 - 1$		$\mathrm{J}(X)$ simple with endomorphism algebra $\mathbb{Q}(\zeta_7)$
U_6	$x(x^6 + 1)$	$I = [1, 1, 1]$	$C_1 : y^2 = x^3 + x$, i.e., $j = 1728$
$C_2 \times S_4$	$x^8 + 14x^4 + 1$	$I = [1, 1, 1]$	$C_1 : y^2 = x^3 + x^2 - 4x - 4$, i.e., $j = 2^4 \cdot 3^{-2} \cdot 13^3$
U_8	$x^8 + 1$	$I = [1, 2, 2]$	$\begin{cases} C_1 : & y^2 = x^4 + 1, \text{ i.e., } j = 1728 \\ C_2 : & y^2 = x^4 - 4x^2 + 2, \text{ i.e., } j = 2^6 \cdot 5^3 \end{cases}$

Table: Decomposition of Jacobian: hyperelliptic case

Automorphisms strategy: $g = 3$.

Non-hyperelliptic genus 3 curves stratification by automorphisms



Automorphisms strategy: $g = 3$.

G	$X : F(x,y,z) = 0$	$\mathrm{J} \sim \prod_{i \in I} \mathrm{J}(C_i)$	Curves C_i
C_2	$x^4 + y^4 + z^4 + rx^2y^2 + sy^2z^2 + tz^2x^2$	$I = [1,2,3]$	RR $\begin{cases} C_1 : y^2 = (\frac{r^2}{4} - 1)x^4 + (1/2rs - t)x^2 + (\frac{s^2}{4} - 1) \\ C_2 : y^2 = (\frac{s^2}{4} - 1)x^4 + (1/2st - r)x^2 + (\frac{t^2}{4} - 1) \\ C_3 : y^2 = (\frac{t^2}{4} - 1)x^4 + (1/2tr - s)x^2 + (\frac{r^2}{4} - 1) \end{cases}$
C_3	$x^3z + y(y-z)(y-rz)(y-sz)$		$\mathrm{J}(X)$ generically simple with endomorphism algebra $\mathbb{Q}(\sqrt{-3})$
D_4	$x^4 + y^4 + z^4 + rx^2yz + sy^2z^2$	$I = [1,2,2]$	$\begin{cases} C_1 : y^2 = x^4 + (r^2/4 - s)x^2 + 1, \\ C_2 : y^2 = (-s - 2 + r^2/4)x^4 - 2rx^2 - s + 2 \end{cases}$
S_3	$x(y^3 + z^3) + y^2z^2 + rx^2yz + sx^4$	$I = [1,1,2]$	$\begin{cases} C_1 : y^2 = -x^3 + 9/4x^2 - 3/2rx + r^2/4 - s \\ C_2 : y^2 = x^4 + 2rx^3 + (r^2 - 4s)x^2 - sx \end{cases}$
C_6	$x^3z + y^4 + ry^2z^2 + z^4$	$I = [1,2]$	RR
G_{16}	$x^4 + y^4 + z^4 + ry^2z^2$	$I = [1,2,2]$	$\begin{cases} C_1 : \ y^2 = x^4 - rx^2 + 1 \\ C_2 : \ y^2 = (-r-2)x^4 - r + 2 \end{cases}$
S_4	$x^4 + y^4 + z^4 + r(x^2y^2 + y^2z^2 + z^2x^2)$	$I = [1,1,1]$	$C_1 : y^2 = (\frac{r^2}{4} - 1)x^4 + (\frac{r^2}{2} - r)x^2 + (\frac{r^2}{4} - 1)$
C_9	$x^3y + y^3z + z^4$		$\mathrm{J}(X)$ simple with endomorphism algebra $\mathbb{Q}(\zeta_9)$
G_{48}	$x^4 + (y^3 - z^3)z$	$I = [1,2,2]$	$\begin{cases} C_1 : \ y^2 = x^3 + 1 \\ C_2 : \ y^2 = x^3 + x \end{cases}$
G_{96}	$x^4 + y^4 + z^4$	$I = [1,1,1]$	$C_1 : y^2 = x^3 + x$
G_{168}	$x^3y + y^3z + z^3x$	$I = [1,1,1]$	$C_1 : y^2 + xy + y = x^3 - x^2 - 2680x + 66322$, i.e., $j = -3375$

Table: Decomposition of the Jacobian: non-hyperelliptic case

The idea

Take a degree d_y morphisms $Y \to \mathbb{P}^1$, consider the composition $X \to Y \to \mathbb{P}^1$ with the degree d_X morphism $X \to Y$, and call Z the curve corresponding to the Galois closure of the corresponding function field extensions.

$$Z \to X \to Y \to \mathbb{P}^1$$

The idea

Take a degree d_y morphisms $Y \to \mathbb{P}^1$, consider the composition $X \to Y \to \mathbb{P}^1$ with the degree d_X morphism $X \to Y$, and call Z the curve corresponding to the Galois closure of the corresponding function field extensions.

$$Z \to X \to Y \to \mathbb{P}^1$$

Question: Can we find the Prym variety $\mathrm{Prym}(X/Y)$ as the Jacobian of a curve in the diagram $Z \to \mathbb{P}^1$?

The idea

Take a degree d_y morphisms $Y \to \mathbb{P}^1$, consider the composition $X \to Y \to \mathbb{P}^1$ with the degree d_X morphism $X \to Y$, and call Z the curve corresponding to the Galois closure of the corresponding function field extensions.

$$Z \to X \to Y \to \mathbb{P}^1$$

Question: Can we find the Prym variety $\mathrm{Prym}(X/Y)$ as the Jacobian of a curve in the diagram $Z \to \mathbb{P}^1$?

- Not necessarily. But when? and how to check it?

Example: the RR construction.

Let us take $g(X) = 3$, $g(Y) = 1$ and $d = 2$ with 4 ramification points: Q_1, Q_2, Q_3 and Q_4.

We choose $Y \to \mathbb{P}^1$ of degree 2 collapsing the first 2: quotient by the involution $P \mapsto Q_1 + Q_2 - P$.

Example: the RR construction.

Let us take $g(X) = 3$, $g(Y) = 1$ and $d = 2$ with 4 ramification points: Q_1, Q_2, Q_3 and Q_4.

We choose $Y \to \mathbb{P}^1$ of degree 2 collapsing the first 2: quotient by the involution $P \mapsto Q_1 + Q_2 - P$.

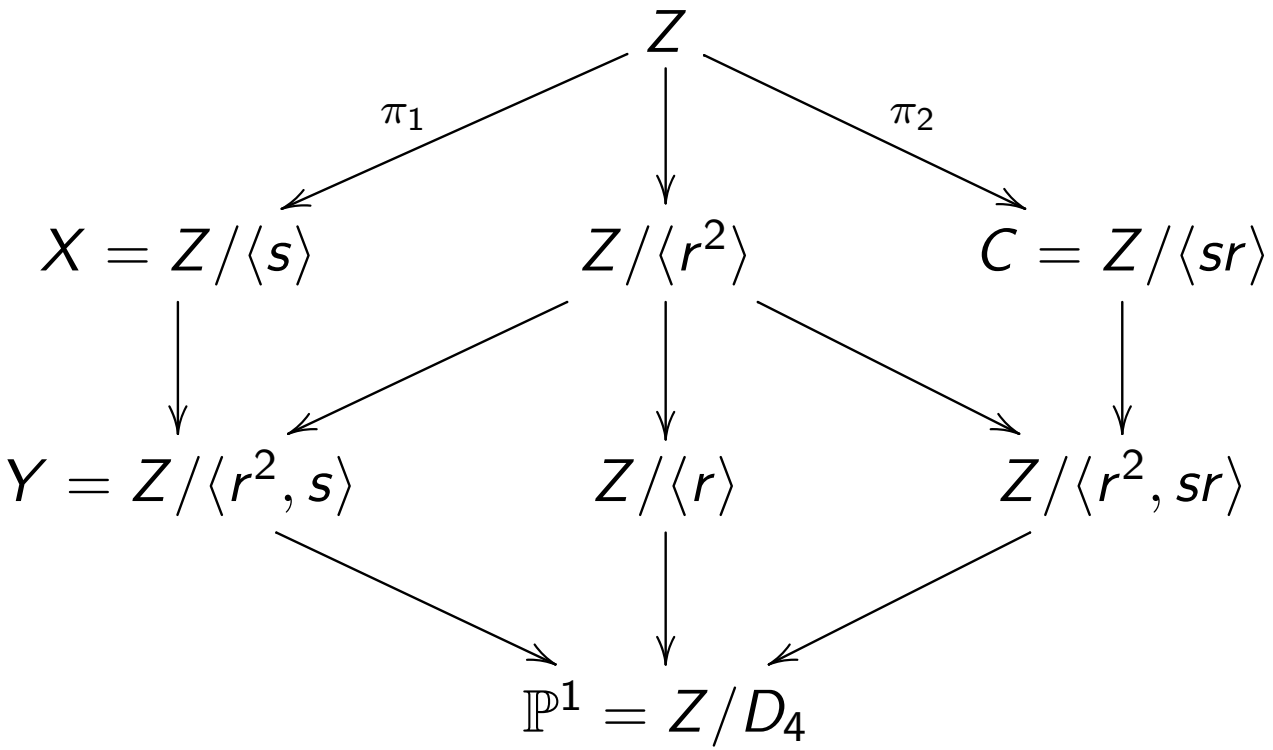
Then $Y : y^2 = f(t) = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)$ and

$$X : \begin{cases} y^2 = & f(t) \\ x^2 = & (t - \beta)(p_2(t) + y) \end{cases}$$

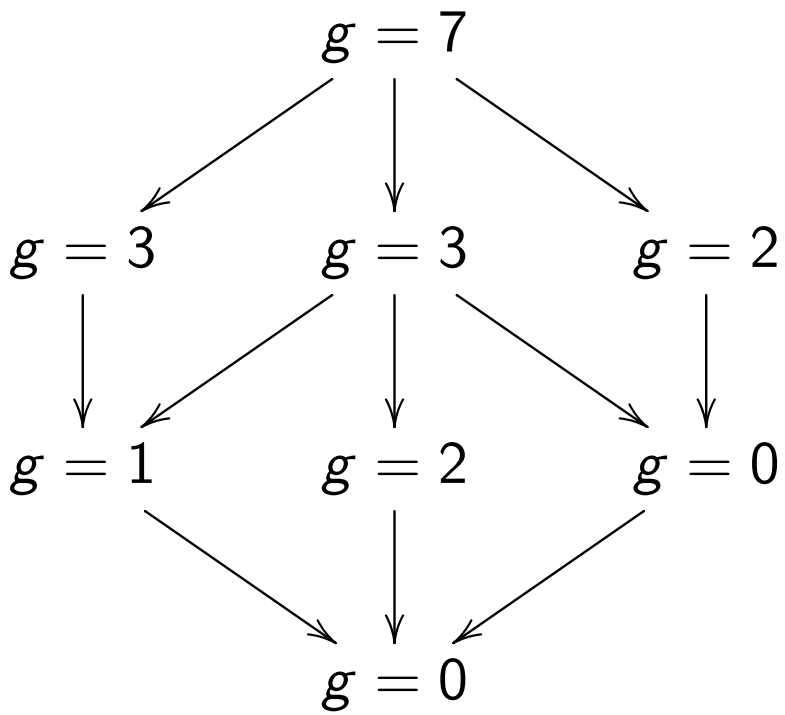
where p_2 is a polynomial of degree 2 and $p_2(t)^2 - f(t) = t(t - \gamma)p_1(t)^2$ with $p_1(t)$ a polynomial of degree 1.

The Galois group of $Z \to \mathbb{P}^1$ is D_4.

Example: the RR construction.



Example: the RR construction.



Example: the RR construction.

Equations for the genus 2 curve:

$$C = \begin{cases} v^2 = 2(t-\beta)(p_2(t) + wp_1(t)), \\ w^2 = t(t-\gamma) \end{cases}$$

Parametrizing the conic:

$$s^2 = 2\left(\gamma - \beta(1-u^2)\right)\left((1-u^2)^2 p_2\left(\frac{\gamma}{1-u^2}\right) + \gamma u(1-u^2) p_1\left(\frac{\gamma}{1-u^2}\right)\right).$$

Example: the RR construction.

Theorem

The Jacobian of X decomposes up to isogeny as

$$\mathrm{J}(X) \sim Y \times \mathrm{J}(C).$$

Proof.

It suffices to prove that the subspaces $(\phi\pi_1)^* H^0(Y, \Omega^1_Y)$ and $\pi_2^* H^0(C, \Omega^1_C)$ generate the space $\pi_1^* H^0(X, \Omega^1_X)$. □

Lemma

Write $H^0(Z, \Omega^1_Z) \cong (1)^{\oplus e_0} \oplus V_1^{\oplus e_1} \oplus V_2^{\oplus e_2} \oplus V_3^{\oplus e_3} \oplus (2)^{\oplus e_4}$ as representations of D_4. Then $e_0 = e_3 = 0$, $e_1 = e_4 = 2$ and $e_2 = 1$.

A group theoretic algorithm

Theorem (Miranda)

Let Y be a compact Riemann surface, B be a finite subset of Y, and let q be a base point of $Y \setminus B$. There is a bijection

$$\left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{holomorphic maps } \varphi : X \to Y \\ \text{of degree } d \\ \text{whose branch points} \\ \text{lie in } B \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{group homomorphisms} \\ \rho : \pi_1(Y \setminus B, q) \to S_d \\ \text{with transitive image} \\ \text{up to conjugacy in } S_d \end{array} \right\}$$

denoted by $\varphi_\rho \leftrightarrow \rho$ and $\varphi \leftrightarrow \rho_\varphi$. If γ_i is a small loop based at q around $b_i \in B$, the ramification structure of φ_ρ at b_i is the cycle type of $\sigma_i := \rho([\gamma_i])$.

A group theoretic algorithm

Theorem (Miranda)

There is a bijective correspondence

$$\left\{\begin{array}{c}\text{isomorphism classes of}\\ \text{holomorphic maps } \varphi : C \to \mathbb{P}^1\\ \text{of degree } d\\ \text{whose branch points}\\ \text{lie in } B\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{conjugacy classes of } n\text{-tuples}\\ (\sigma_1, \ldots, \sigma_n) \text{ of permutations in } S_d\\ \text{such that } \sigma_1 \cdots \sigma_n = 1\\ \text{and the subgroup generated by the } \sigma_i\\ \text{is transitive}\end{array}\right\}$$

which enjoys the following additional property: the ramification structure at b_i of the map φ corresponding to $(\sigma_1, \ldots, \sigma_n)$ is the cycle type of σ_i.

A group theoretic algorithm

The genus of the quotients Z/H are computed with Riemann-Hurwitz.

Theorem (Chevalley-Weil)

Let $\varphi : Z \to \mathbb{P}^1$ be a branched Galois cover of smooth projective complex algebraic curves, let B be its branch locus, and let G be the corresponding Galois group. Let τ_χ be an irreducible linear complex representation of G with character $\chi : G \to \mathbb{C}$ and define e_i and $N_{i,\alpha} := N_{i,\alpha}(\tau_\chi)$ as above. The multiplicity ν_χ of τ_χ in the G-representation $H^0(Z, \Omega^1_Z)$ is given by

$$\nu_\chi = -d_\chi + \sum_{i=1}^{p} \sum_{\alpha=0}^{e_i-1} N_{i,\alpha} \left\langle -\frac{\alpha}{e_i} \right\rangle + \sigma,$$

where $d_\chi = \chi(1)$ is the dimension of τ_χ and

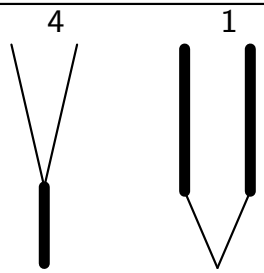
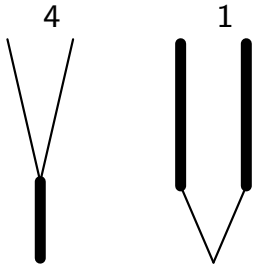
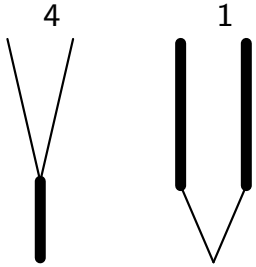
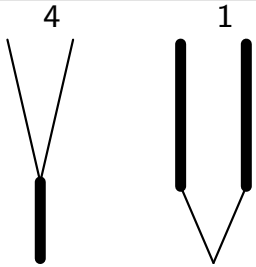
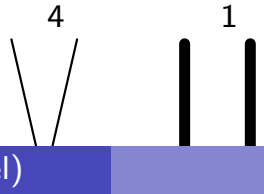
$$\sigma = \begin{cases} 1 \text{ if } \chi \text{ is the trivial character} \\ 0 \text{ otherwise.} \end{cases}$$

A group theoretic algorithm

INPUT: (g_X, g_Y, d_X, d_Y, R), ramification type $X \to \mathbb{P}^1$.
OUTPUT: all the possibilities for (G, H_X, H_Y, Σ).

1. Initialize $d := d_X d_Y$ and let $\mathcal{L}_1$ and $\mathcal{L}_2$ be the empty lists.
2. Loop over representatives G of conjugacy classes of subgroups of S_d. For each representative do:
   1. If G is not transitive, discard G and continue with the next subgroup;
   2. Set H_X to be the stabilizer of 1 in G;
   3. Append to $\mathcal{L}_1$ all sible postriples (G, H_X, H_Y).
3. Using Breuer's algorithm, find all possible isomorphism classes of monodromy data Σ. Loop over these Σ:
   1. Loop over the triples (G, H_X, H_Y) in $\mathcal{L}_1$;
   2. Compute the genera of Z/H_X and of Z/H_Y. If $g(Z/H_X) \neq g_X$ or $g(Z/H_Y) \neq g_Y$, return to the beginning of the loop;
   3. Compute the ramification structure of $X \to \mathbb{P}^1$. If it is different from R, return to the beginning of the loop;
   4. Add (G, H_X, H_Y, Σ) to $\mathcal{L}_2$.
4. Return $\mathcal{L}_2$.

The results

Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \to C_i$
g2-2	2, 1, 2		4, 2	[0,0],[4,0]	[1]	[2]
g2-3	2, 1, 3		12, 4	[0,0],[16,0]	[1]	[2]
g2-4	2, 1, 4		48, 13	[0,0],[48,0]	[1]	[4]
g2-5	2, 1, 5		240, 61	[0,0],[160,0]	[1]	[12]
g2-6	2, 1, 6		1440, 361	[0,0],[240,0]	[1]	[48]

The results

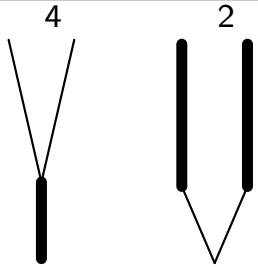
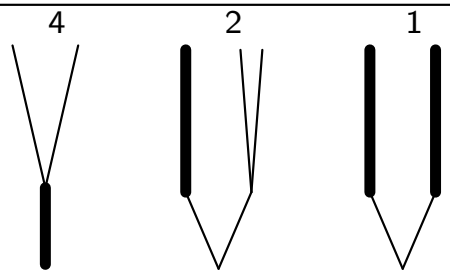
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \to C_i$
`rr-spec`	3, 1, 2		4, 3	[3, 0], [0, 0]	[1, 1]	[2]
`rr-gen`	3, 1, 2		8, 7	[8, 0], [0, 0]	[2]	[2]

Table: Recovering Ritzenthaler–Romagny

The results

Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \to C_i$
3-orig	5, 3, 2		24, 37	[?, 0], [0, 0]	[2]	[6]
3-g7	7, 4, 2		24, 49	[?, 0], [0, 0]	[2]	[6]
3-g9	9, 5, 2		24, 61	[?, 0], [0, 0]	[2]	[6]
3-g11	11, 6, 2		24, 73	[?, 0], [0, 0]	[2]	[6]

Table: Generalizing Bruin's results

The results

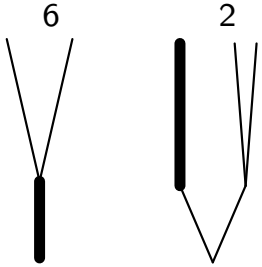
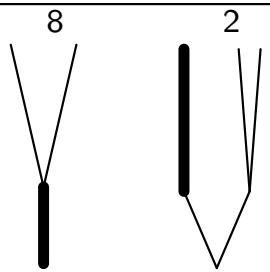
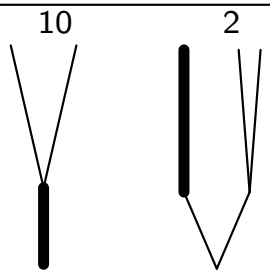
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \to C_i$
g2	4, 2, 2	6 2 	8, 9	[32, 0], [0, 0]	[2]	[2]
g3	6, 3, 2	8 2 	8, 13	[128, 0], [0, 0]	[3]	[2]
g4	8, 4, 2	10 2 	8, 17	[512, 0], [0, 0]	[4]	[2]

Table: Testing Dalaljan's results

The results

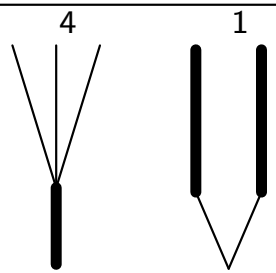
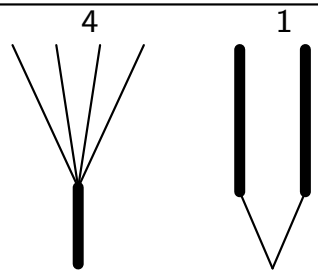
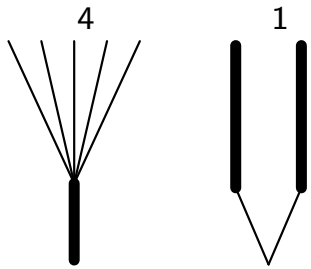
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	deg Z
`total-3`	3, 1, 3		6, 3 12, 5	[9, 0], [0, 0] [0, 0], [6, 0]	[2] [2]	[2 [2
`total-4`	4, 1, 4		48, 19	[48, 0], [16, 0]	[3], [3]	[8],
`total-5`	5, 1, 5		10, 5 20, 9 100, 41 120, 49 120, 49 200, 81 240, 97 7200, 2881 14400, 5761	[25, 0], [0, 0] [0, 0], [12, 0] [0, 12], [0, 0] [380, 0], [0, 0] [0, 0], [0, 25] [0, 96], [0, 0] [0, 450], [0, 60] [0, 90], [0, 0] [0, 360], [0, 0]	[4] [2] [2] or [1]	[2 [2 [24]

Table: Merging total ramification above two points

Some equations: special case $g_X = k$, $g_Y = 1$, $d_x = 2$.

Let $Z : y^2 = f(x) = x^{4k} + ax^{3k} + bx^{2k} + ax^k + 1$ be a hyperelliptic curve.
The group $\mathrm{Aut}(Z)$ contains the hyperelliptic involution $\iota(x, y) = (x, -y)$ and the elements $\sigma(x, y) = (\zeta_k x, y)$ and $\tau(x, y) = (\frac{1}{x}, \frac{y}{x^{2k}})$.
- The quotient $\pi_{Z/X} : Z \to X := Z/\langle \iota\tau \rangle$ (described thanks to $u = x + \frac{1}{x}$ and $v = \frac{y}{x^k}(x - \frac{1}{x})$), is a smooth hyperelliptic curve of genus k with equation

$$X : v^2 = (u^2 - 4)(g^2(u) + ag(u) + b - 2).$$

- The quotient $\pi_{Z/C} : Z \to C := Z/\langle \tau \rangle$ is a hyperelliptic curve C of genus $k - 1$. Via $u = x + \frac{1}{x}$ and $w = \frac{y}{x^k}$, it is given by $C : w^2 = g^2(u) + ag(u) + b - 2$.
- The quotient $\pi_{X/Y} : X \to Y = Z/\langle \iota\tau, \sigma \rangle$ is an elliptic curve. Via $U = x^k + \frac{1}{x^k}$ and $V = \frac{y}{x^k}(x^k - \frac{1}{x^k})$, we get the equation $Y : V^2 = (U^2 - 4)(U^2 + aU + b - 2)$.

Proposition

With the notation above, the Prym variety $\mathrm{Prym}(X/Y)$ *is isogenous to the Jacobian of the curve* C.

Thank you for your attention!
Questions?