Computation of Richelot isogeny chains

Sabrina Kunzweiler
Ruhr-Universität Bochum

December 14, 2022

Talk at the Workshop Ciao 2022.

Genus-2 curves and their Jacobians

Genus-2 curves

A **genus-**2 **curve** $\mathcal{C}$ over a field K with $char(K) \neq 2$ is a curve defined by an equation of the form

$$\mathcal{C} : y^2 = f(x),$$

where $f \in K[x]$ is a square-free polynomial of degree 5 or 6.

We call $y^2 = f(x)$ a **hyperelliptic equation** for $\mathcal{C}$.

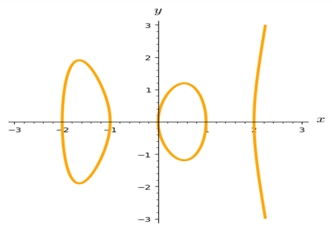


Figure 1: $y^2 = x(x^2 - 1)(x^2 - 4)$

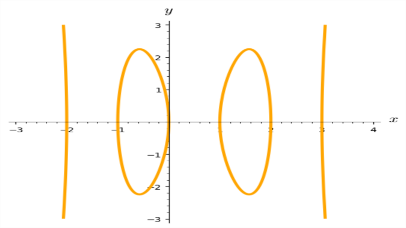


Figure 2: $y^2 = x(x^2 - 1)(x^2 - 4)(x - 3)$

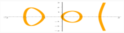
Hyperelliptic Equations

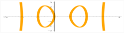
- A coordinate transformation

$$t : x \mapsto x' = \frac{ax+b}{cx+d},\; y \mapsto y' = \frac{ey}{(cx+d)^3}$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(K),\; e \in K \setminus \{0\}$ allows to move between different hyperelliptic equations.

We introduce two types of hyperelliptic equations:

Type 1: $y^2 = E\,x(x^2 - Ax + 1)(x^2 - Bx + C)$ 

Type 2: $y^2 = (x^2 - 1)(x^2 - A)(Ex^2 - Bx + C)$ 

with coefficients $A, B, C, E \in K$.

- ➤ The existence of Type-1 and Type-2 equations over K is equivalent.
- ➤ For $\mathcal{C} : y^2 = f(x)$ over a finite field K: If f splits over K, then $\mathcal{C}$ admits equations of Type 1 and 2.

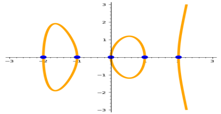
Points of genus-2 curves

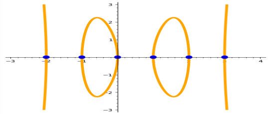
The **set of points** of a hyperelliptic curve $\mathcal{C} : y^2 = f(x)$ is given by

$$\mathcal{C}(\bar{K}) = \underbrace{\{(u,v) \in \bar{K}^2 \mid v^2 = f(u)\}}_{\text{affine points}} \cup \underbrace{\begin{cases} \{\infty\} & \text{if } \deg(f) = 5 \\ \{\infty_+, \infty_-\} & \text{if } \deg(f) = 6 \end{cases}}_{\text{point(s) at infinity}}.$$

The **Weierstrass points** of $\mathcal{C}$ are the points fixed by the hyperelliptic involution τ, defined as $\tau(u,v) = (u,-v)$ and $\tau(\infty_\pm) = \infty_\mp$, resp. $\tau(\infty) = \infty$.

- Every genus-2 curve has precisely 6 Weierstrass points.





❗ In contrast to elliptic curves, the set $\mathcal{C}(\bar{K})$ is **not** a group.

We write $\mathcal{J}(\mathcal{C})$ for the **Jacobian variety** of a genus-2 curve.

- It is a a principally polarized abelian variety of dimension 2.
- As groups: $\mathcal{J}(\mathcal{C})(L) = Pic^0_{\mathcal{C}}(L)$ for any field extension L/K.
- Any $R \in \mathcal{J}(\mathcal{C})$ has a unique presentation $R = [P_1 + P_2 - D_\infty]$, where $P_1, P_2 \in \mathcal{C}(\bar{K})$ with $\tau(P_1) \neq \tau(P_2)$ and
$$D_\infty = \begin{cases} 2 \cdot \infty & \text{if } \deg(f) = 5, \\ \infty_+ + \infty_- & \text{if } \deg(f) = 6. \end{cases}$$

Mumford presentation

$R = J(a, b)$

For $P_1 = (u_1, v_1), P_2 = (u_2, v_2)$, define $a = (x - u_1)(x - u_2)$ and $b = b_1 x + b_0$ so that $b(u_1) = v_1$ and $b(u_2) = v_2$.

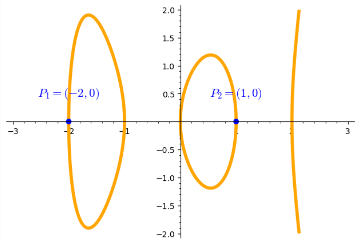


Figure 3: Element $J(x^2 + x - 2, 0)$

Isogenies of Jacobians of genus-2 curves

Torsion elements

Consider $\mathcal{C} : y^2 = f(x)$ over a finite field K with $char(K) = p$.

- $\mathcal{J}(\mathcal{C})[m] \cong (\mathbb{Z}/m\mathbb{Z})^4$ for $m \in \mathbb{N}$ with $p \nmid m$.
- The **Weil pairing**

$$e_m : \mathcal{J}(\mathcal{C})[m] \times \mathcal{J}(\mathcal{C})[m] \to \boldsymbol{\mu}_m.$$

  is a bilinear, alternating pairing.

Example: $m = 2$, $f = \prod_{i=1}^{6}(x - r_i)$

- $\mathcal{J}(\mathcal{C})[2] \setminus \{0\} = \{J\left((x - r_i)(x - r_j), 0\right) \mid i \neq j\}$.
  $\Rightarrow$ Correspondence between pairs of Weierstrass points of $\mathcal{C}$ and 2-torsion elements of $\mathcal{J}(\mathcal{C})$.
- $e_2\left(J\left((x - r_i)(x - r_j), 0\right), J\left((x - r_k)(x - r_l), 0\right)\right)$
  $= \begin{cases} -1 & \text{if } \mid \{i,j\} \cap \{k,l\} \mid = 1, \\ 1 & \text{otherwise.} \end{cases}$

General isogenies

Consider $\mathcal{J}(\mathcal{C})$ over K with $char(K) = p$ and let $\ell \neq p$ prime.

- An (ℓ, ℓ)-**isogeny** is an isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{A} = \mathcal{J}(\mathcal{C})/G$, [1] where $G \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ and $e_{\ell_{|G}} \equiv id$.
  $\Rightarrow G$ is called maximal ℓ-isotropic.
- Non-backtracking composition of (ℓ, ℓ)-isogenies:
  $$\mathcal{J}(\mathcal{C}) \to \mathcal{A}_1 \to \cdots \to \mathcal{A}_n.$$
  For $G = \ker(\mathcal{J}(\mathcal{C}) \to \mathcal{A}_n)$, we have that $e_{\ell^n{}_{|G}} = id$ and $G \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^{n-k}\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z}$ for some $0 \leq k \leq n/2$.
  $\Rightarrow G$ is called maximal ℓ^n-isotropic.
- An (ℓ^n, ℓ^n)-**isogeny** is an isogeny as above, where $k = 0$, i.e. $G \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$.

[1] In general, $\mathcal{A}$ is a principally polarized abelian surface. In most cases this is again the Jacobian of a genus-2 curve $\mathcal{C}'$.

Richelot Isogenies

Let $\mathcal{C} : y^2 = g_1(x)g_2(x)g_3(x)$ with $g_i = g_{2,i}x^2 + g_{1,i}x + g_{0,i}$ and write $\delta = \det\left((g_{i,j})_{i,j}\right)$.

- The group $G = \langle J(g_1, 0), J(g_2, 0)\rangle = \{0, J(g_1, 0), J(g_2, 0), J(g_3, 0)\}$ is maximal 2-isotropic.
- If $\delta \neq 0$, then $\mathcal{J}(\mathcal{C})/G = \mathcal{J}(\mathcal{C}')$, where

$$\mathcal{C}' : y^2 = h_1(x)h_2(x)h_3(x) \quad \text{with } h_i = \delta^{-1}(g'_{i+1}g_{i+2} - g_{i+1}g'_{i+2}).$$

- The isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ is called **Richelot isogeny** and it is defined by the correspondence

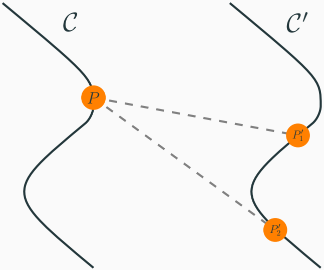
$$\begin{aligned} \mathcal{R} : \quad 0 &= g_1(u)h_1(u') + g_2(u)h_2(u') \\ vv' &= g_1(u)h_1(u')(u - u') \end{aligned}$$

for points $(P, P') = ((u, v), (u', v')) \in \mathcal{C} \times \mathcal{C}'$.

Richelot correspondence

Recall $\mathcal{R} \subset \mathcal{C} \times \mathcal{C}'$.

$$\mathcal{R}: \quad 0 = g_1(u)h_1(u') + g_2(u)h_2(u')$$
$$vv' = g_1(u)h_1(u')(u - u').$$



The correspondence induces a map $\mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$:

$$[P + Q - D_\infty] \mapsto \underbrace{[P_1 + P_2 + Q_1 + Q_2 - 2D'_\infty]}_{\text{unreduced representation}} = [P' + Q' - D'_\infty].$$

Richelot Isogeny Chains

Our Algorithm

Setup: A genus-2 curve

$$\mathcal{C} : y^2 = (x^2 - 1)(x^2 - A)(Ex^2 - Bx + C)$$

and a (special) symplectic basis (B_1, B_2, B_3, B_4) for $\mathcal{J}(\mathcal{C})[2^n]$.

Input: $a, b, c \in \mathbb{Z}/2^n\mathbb{Z}$ defining $G = \langle B_1 + aB_3 + bB_4,\ B_2 + bB_3 + cB_4\rangle$.

Output: $\mathcal{J}(\mathcal{C}') = \mathcal{J}(\mathcal{C})/G$. ❗

❗ Restriction in our work: We will only consider isogenies where the codomain is again the Jacobian of a hyperelliptic curve. In general, one could also have $\mathcal{J}(\mathcal{C})/G = \mathcal{E}_1 \times \mathcal{E}_2$ for two elliptic curves $\mathcal{E}_1, \mathcal{E}_2$.

Our Algorithm

Computation of $\mathcal{J}(\mathcal{C})/G$ with $G = \langle J_1, J_2 \rangle \subset \mathcal{J}(\mathcal{C})[2^n]$.

General outline: Composition of n Richelot isogenies

$$\mathcal{J}_0 = \mathcal{J}(\mathcal{C}_0) \xrightarrow{\phi_1} \mathcal{J}_1 = \mathcal{J}(\mathcal{C}_1) \xrightarrow{\phi_2} \mathcal{J}_2 = \mathcal{J}(\mathcal{C}_2) \longrightarrow \quad \dots \xrightarrow{\phi_n} \mathcal{J}_n = \mathcal{J}(\mathcal{C}_n).$$

$$\psi_2 : \mathcal{J}_0 \dashrightarrow \mathcal{J}_2$$

where $\ker(\phi_i) = \langle 2^{n-i}\psi_{i-1}(J_1), 2^{n-i}\psi_{i-1}(J_2) \rangle$.

Step i:

- transformation to Type-1 equation with special kernel form
- $\hat{\phi}_i$: application of our $(2,2)$-isogeny formula

$$\begin{array}{ccc} \mathcal{J}_{i-1} = \mathcal{J}(\mathcal{C}_{i-1}) & \overset{\phi_i}{\dashrightarrow} & \mathcal{J}_i = \mathcal{J}(\mathcal{C}_i) \\ \downarrow \wr & \nearrow_{\hat{\phi}_i} & \\ \mathcal{J}'_{i-1} = \mathcal{J}(\mathcal{C}'_{i-1}) & & \end{array}$$

$(2,2)$-isogeny formula

Theorem (K.)
Let $\mathcal{C} : y^2 = Ex(x^2 - Ax + 1)(x^2 - Bx + C)$ with $C \neq 1$ and $G = \langle J(x, 0), J\left(x^2 - Ax + 1, 0\right)\rangle \subset \mathcal{J}(\mathcal{C})[2]$.

- Then $\mathcal{J}(\mathcal{C})/G = \mathcal{J}(\mathcal{C}')$ with

$$\mathcal{C}' : y^2 = (x^2 - 1)(x^2 - A')(E'x^2 - B'x + C'),$$

  where $A' = C$, $B' = \frac{2}{E}$, $C' = \frac{B-AC}{E(1-C)}$, $E' = \frac{A-B}{E(1-C)}$.
- We provide explicit formulas for the $(2,2)$-isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$. I.e. expressions $a_i', b_i' \in K[A, B, C, E, a_0, a_1, a_2, b_0, b_1]$ so that

$$\phi(J(a_2x^2+a_1x+a_0, b_1x+b_0)) = J(a_2'x^2+a_1'x+a_0', b_1'x+b_0') \in \mathcal{J}(\mathcal{C}').$$

Transformation

Goal: Given $\mathcal{C} : y^2 = f(x)$, a $(2,2)$-group $\langle J(g_1, 0), J(g_2, 0)\rangle$ and a $R \in \mathcal{J}(\mathcal{C})$ with $2 \cdot R = J(g_1, 0)$:
find a transformation $t : (x, y) \mapsto (x', y')$ so that

- $\mathcal{C}' : {y'}^2 = Ex'({x'}^2 - Ax' + 1)(E{x'}^2 - Bx' + C)$.
- $t(g_1) = x'$ and $t(g_2) = {x'}^2 - Ax' + 1$.

Step 1: Factorize $g_1(x) = (x - \alpha_1)(x - \alpha_2)$, $g_2(x) = (x - \beta_1)(x - \beta_2)$
(Note: no square-root computations necessary due to the special setup).

Step 2: Set $\hat{t} : x \mapsto \hat{x} = \frac{x-\alpha_2}{x-\alpha_1}$, $y \mapsto \hat{y} = \frac{y}{(x-\alpha_1)^3}$ and compute
$\hat{\mathcal{C}} : \hat{y}^2 = c_f \cdot \hat{x}(\hat{x} - \hat{\beta}_1)(\hat{x} - \hat{\beta}_2)(\hat{x} - \hat{\gamma_1})(\hat{x} - \hat{\gamma}_2)$.

Step 3: Compute $a \in K$ such that satisfies $a^2 = \frac{1}{\hat{\beta}_1\hat{\beta}_2}$.
Set $t : x \mapsto x' = a \cdot \frac{x-\alpha_2}{x-\alpha_1}$, $y \mapsto y' = \frac{y}{(x-\alpha_1)^3}$.

➤ How to compute $\sqrt{\hat{\beta}_1\hat{\beta}_2}$? ➤ Why is it in K?

Division by 2 (Zarhin, 2016)

Let $\mathcal{C} : y^2 = g(x)$ with $g = c_g(x - r)\prod_{i=1}^{4}(x - r_i)$ and $P = (r, 0)$.

Then any choice of square roots

$$\mathfrak{r} = (\mathfrak{r}_1, \ldots, \mathfrak{r}_4) \in \bar{K}^4 \quad \text{with } \mathfrak{r}_i^2 = r - r_i \quad \text{for } i \in \{1, 2, 3, 4\}$$

defines a 4-torsion point $J(a_\mathfrak{r}, b_\mathfrak{r}) \in \mathcal{J}(\mathcal{C})$ with $2 \cdot J(a_\mathfrak{r}, b_\mathfrak{r}) = J(x - r, 0)$, where

$$a_\mathfrak{r} = (x - r)^2 - s_2(\mathfrak{r})(x - r) + s_4(\mathfrak{r}),$$

$$\frac{1}{\sqrt{c_g}} \cdot b_\mathfrak{r} = (s_1(\mathfrak{r})s_2(\mathfrak{r}) - s_3(\mathfrak{r}))(x - r) - s_1(\mathfrak{r})s_4(\mathfrak{r})$$

with s_i the i-th elementary symmetric polynomial in $\mathfrak{r} = (\mathfrak{r}_1, \ldots, \mathfrak{r}_4)$.

Computing $\sqrt{\beta_1\beta_2}$

Proposition (K.)
Let $\mathcal{C} : y^2 = c_f x(x-\beta_1)(x-\beta_2)(x-\gamma_1)(x-\gamma_2)$. If $R = J(x^2 + a_1 x + a_0, b_1 x + b_0) \in \mathcal{J}(\mathcal{C})(K)$ satisfies $2 \cdot R = J(x, 0)$, then

$$\sqrt{\beta_1\beta_2} = \frac{(a_0 b_0 b_1 - a_1 b_0^2)\beta_1\beta_2 + c_g a_0^2 (a_0 - \beta_1\beta_2)^2}{b_0^2\beta_1\beta_2 + c_g a_0^2(a_0 - \beta_1\beta_2)(-a_1 - \beta_1 - \beta_2)}$$

Proof.

- Set $r = 0$ and $\mathfrak{r} = (\sqrt{-\beta_1}, \sqrt{-\beta_2}, \sqrt{-\gamma_1}, \sqrt{-\gamma_2})$.
- Extract $s_i(\mathfrak{r})$ from the Mumford coordinates of R.
- Use that $\mathfrak{r}_1\mathfrak{r}_2 = \frac{s_1(\mathfrak{r})s_3(\mathfrak{r})\mathfrak{r}_1^2\mathfrak{r}_2^2 + (s_4(\mathfrak{r}) - \mathfrak{r}_1^2\mathfrak{r}_2^2)^2}{\mathfrak{r}_1^2\mathfrak{r}_2^2 s_1(\mathfrak{r})^2 + (s_4(\mathfrak{r}) - \mathfrak{r}_1^2\mathfrak{r}_2^2)(s_2(\mathfrak{r}) + \mathfrak{r}_1^2 + \mathfrak{r}_2^2)}$.

$\square$

Performance

We compare our algorithm to other implementations on a typical G2SIDH instance with $\log(p) \approx 100$ and compute a $(2^{51}, 2^{51})$-isogeny.

	pure isogeny	with image points
Genus-2 SIDH [FT '19]	72	127
SIDH-Attack [CD '22]	0.16	0.26
↳ sagemath [PO '22]	0.4	0.6
This work	0.06	0.08
↳ sagemath	0.17	0.23

Table 1: Runtime in seconds on a laptop with Intel i7-8565U processor

Code and verification of all formulas:
`https://github.com/sabrinakunzweiler/richelot-isogenies`

Richelot Isogeny Chains on the Kummer Surface

Kummer Surface

For a genus-2 curve $\mathcal{C} : y^2 = f(x)$, the **Kummer surface** is defined as $\mathcal{K}(\mathcal{C}) = \mathcal{J}(\mathcal{C})/\langle \pm 1 \rangle$.

- Quartic surface in $\mathbb{P}^3$.
- 16 singular points corresponding to the 2-torsion points of $\mathcal{J}(\mathcal{C})$.
- Quotient map: $\xi : \mathcal{J}(\mathcal{C}) \to \mathcal{K}(\mathcal{C})$,
  $[(x_1, y_1) + (x_2, y_2) - D_\infty] \mapsto [1 : x_1 + x_2 : x_1 x_2 : \frac{\phi(x_1,x_2) - 2y_1 y_2}{(x_1 - x_2)^2}]$,
  where ϕ is a polynomial depending on f.

Example:
Let $\mathcal{C} : y^2 = (x^2 - 1)(x^2 - A)(x^2 - Bx + C)$ be Type-2, then

- $\mathcal{K}(\mathcal{C}) : \left(\xi_1^2 - 4\xi_0\xi_2\right) \cdot \xi_3^2 - 2\left((2C\xi_0 - B\xi_1 + 2E\xi_2)(-A\xi_0 + \xi_2)(-\xi_0 + \xi_2)\right) \cdot \xi_3$ $+\psi(\xi_0, \xi_1, \xi_2)$.
- $\xi : J(x^2 - 1, 0) \mapsto [1 : 0 : -1 : (A+1)(C - E)]$,
  $\xi : J(x^2 - A, 0) \mapsto [1 : 0 : -A : (A+1)(C - AE)]$.

Richelot Isogeny on the Kummer Surface

Proposition (K.)
Let $\mathcal{C} : y^2 = (x^2-1)(x^2-A)(Ex^2-Bx+C)$ with $B \neq 0$ and $G = \langle J\left(x^2-1,0\right), J\left(x^2-A,0\right)\rangle \subset \mathcal{J}(\mathcal{C})[2]$.

- Then $\mathcal{J}(\mathcal{C})/G = \mathcal{J}(\mathcal{C}')$ with $\mathcal{C}' : y^2 = E'x(x^2-A'x+1)(x^2-B'x+C')$ and $A' = 2\frac{E+C}{B},\ B' = 2\frac{AE+C}{B},\ C' = A,\ E' = 2B.$
- We provide explicit formulae for the induced map $\phi : \mathcal{K}(\mathcal{C}) \to \mathcal{K}(\mathcal{C}')$.

```
def KummerRichelot(coefficients, point):
        [A,B,C,E] = coefficients
        [x0,x1,x2,x3] = point

        y0 = (A*(E-C) - C)*x0^2 + C*x1^2 - B*x1*x2 + E*x2^2 + x0*x3
        y1 = A*B*x0^2 -2 (A*(C + E) + C)*x0*x1 + 2(A*E + C)*(C + E)/B*x1^2
        + B*(A + 1)*x0*x2 - 2*(A*E + C - E)*x1*x2 + B*x2^2 + x1*x3
        y2 = A*C*x0^2 - A*B*x0*x1 + A*E*x1^2 - (A*E - C + E)*x2^2 + x2*x3
        y3 = (A^2*(4*E^2 - B^2) - A*B^2)*x0^2 + A*B^2*x1^2 + 4*A*(2*C*E - A*B)*x0*x2
        - ((A + 1)*B^2 - 4*C^2)*x2^2 + 4*A*E*x0*x3 + 4*C*x2*x3 + x3^2

        return [y0,y1,y2,y3]
```

Thank you!