PROJECTIVE GEOMETRY OF HESSIAN ELLIPTIC CURVES AND GENUS 2 TRIPLE COVERS OF CUBICS

RÉMY OUDOMPHENG

Abstract. The existence of finite maps from hyperelliptic curves to elliptic curves has been studied for more than a century and their existence has been related to isogenies between a product of elliptic curves and their Jacobian surface [Kuh88, Kan97].

Such finite covers, sometimes named *gluing maps* have recently appeared in cryptography in the context of genus 2 isogenies and more spectacularly, in the work of Castryck and Decru about the cryptanalysis of SIKE [CD22]. Computation methods include the use of algebraic theta functions [CR15, LR] or correspondences such as Richelot isogenies or degree 3 analogues [BHLS15, BFT14, CD21, Kun22, Smi05].

This article aims at giving geometric meaning to the *gluing* morphism from a product of elliptic curves $E_1 \times E_2$ to a genus 2 Jacobian when it is a degree $(3, 3)$ isogeny. An explicit universal family and an algorithm were previously provided in [BHLS15] and a similar special case was studied in [Kuw11].

We provide an alternative construction of the universal family using concepts from classical algebraic and projective geometry. The family of genus 2 curves which are triple covers of 2 elliptic curves with a level 3 structure arises as a correspondence given by a polarity relation.

The construction does not provide closed formulas for the final curves equations and morphisms. However, an alternative algorithm based on the geometric construction is proposed for computation on finite fields. It relies only on elementary operations and a limited number of square roots and computes the equation of the genus 2 curves and morphisms in all cases.

1. Introduction

The Hesse equations are a linear system of plane cubics defined by homogeneous equations in $\mathbb{P}^2$:

$$E_\lambda : x^3 + y^3 + z^3 = 3\lambda xyz$$

They are classically known to provide a model for the universal family of elliptic curves with a rational 3-level structure (the modular curve $\mathcal{X}_0(3)$), with canonical sections for the 3-torsion points at coordinates $[1 : -\zeta^k : 0]$, $[0 : 1 : -\zeta^k]$, $[-\zeta^k : 0 : 1]$, where ζ is a cubic root of unity and $k = 1, 2, 3$.

The 9 torsion points are base points on this pencil and any other point in the plane belongs to a unique member E_λ of the pencil. This identifies the total space of the Hesse pencil with the blow-up of $\mathbb{P}^2$ at these 9 base points, which is a well known elliptic surface.

The Hesse pencil has a large number of properties in projective geometry which can be found in [AD09, Dol12, BM].

Using the traditional concepts of projective duality, we define a degree 3 correspondence between two members of the Hesse pencil which is invariant under diagonal action of $(\mathbb{Z}/3\mathbb{Z})^2$ acting by translation by order 3 points. The quotient of this correspondence is generically a smooth genus 2 curve.

Date: 26 August 2022.

A special case of genus 2 triple covering using a similar construction is presented by M. Kuwata in [Kuw11].

Several special cases (singular covers, triple ramification) will also be illustrated by equivalent geometric properties.

Section 2 provides an overview of the construction of the family of genus 2 triple covers and explains relations with properties already known in the literature [Kuh88, BHLS15]. Section 3 examines the properties of these triple covers with more detail in order to derive equations and computational aspects in section 4, including an alternate construction algorithm (section 4.7).

Many computations were assisted by Sagemath [SAGE] and Singular [DGPS22]. The final implementation given in appendix uses Sagemath as software framework.

2. Projective geometry of Hesse cubics and polar conjugacy

In this section, the base field is assumed to be an algebraically closed field with characteristic different from 2 and 3. Most computational aspects will target the specific case of finite fields but many formulas are defined over $\mathbb{Q}(j, t_1, t_2)$ and can be applied in a broader context.

In this section we briefly recall the definition of the Hesse pencil of cubics and construct a universal family of common triple covers (with arithmetic genus 10) for pairs of elliptic curves. This family is invariant under the action of $(\mathbb{Z}/3\mathbb{Z})^2$ acting globally by universal projective transformations on all fibres, the action being equivalent to translation by 3-torsion elements.

2.1. The Hesse pencil.

The projective properties of the flex points of a plane cubic are beautifully explained in the expository article [BM] and in [Dol12]. Following [Dol12] a *flex point* designates a point P of a smooth plane curve where the tangent line T_P intersects the curve at point P with multiplicity 3.

We are interested in the following theorem:

Theorem 2.1. *Every plane cubic is projectively equivalent to a curve in Hesse normal form where $t^3 \neq 1$.*

$$x^3 + y^3 + z^3 = 3txyz$$

Moreover, if the cubic is defined over a field $\Bbbk$ and possesses 9 rational flex points, this projective equivalence can be realised over $\Bbbk$.

A cubic defined by a Hesse equation has 9 flex points at coordinates $[0 : 1 : \zeta^i]$ (up to cyclic permutation) where $i \in \{0, 1, 2\}$ and ζ is a cubic root of unity.

Any flex point can be used as the origin of an elliptic curve structure where the group law is the *secant* law. The projection from a flex point defines a degree 2 map $E \to \mathbb{P}^1$ and the corresponding hyperelliptic involution.

The usual convention across this article will be to select point $O = [1 : -1 : 0]$ as the distinguished flex point, so that for any point $P = [x : y : z] \in E$ the point $\iota(P) = [y : x : z]$ also belongs to E and $O, P, \iota(P)$ are collinear.

In particular, the involution associated to O can be represented by the projective map $[x : y : z] \mapsto [y : x : z]$. The corresponding 3 ramification points are the intersection of E with the polar line of O, $\ell_O = \{x = y\}$.

This can be realized explicitly by using affine coordinates $u = z/(x+y+tz)$ and $v = (x - y)/(x + y + tz)$. The equation of E_t in these coordinates is:

$$3v^2 = 4(t^3 - 1)u^3 - 9t^2u^2 + 6tu - 1$$

Throughout this article we assume that the equivalence between a Hessian equation and a level 3 structure is given by the choice of $[1 : -1 : 0]$ as the group law origin, and points $[0 : 1 : -1]$ and $[1 : -j : 0]$ as the basis of the 3-torsion subgroup.

This choice determines uniquely the projective transformation from an elliptic curve with a distinguished symplectic basis of the 3-torsion subgroup (assumed to be defined over $\Bbbk$).

2.2. **Properties of triple covers.** Let H be a genus 2 curve with 2 complementary elliptic degree 3 subcovers $H \to E_1$ and $H \to E_2$. Then H defines a degree 3 correspondence between E_1 and E_2 and the associated morphism $E_1 \to \operatorname{Sym}^3 E_2 \to \operatorname{Jac} E_2 \simeq E_2$ is the zero map [Kuh88].

It is also known [Mir85] that any triple cover can be defined as a subscheme of a $\mathbb{P}^1$-bundle $\operatorname{Proj} E$ where E is a rank 2 vector bundle on the base curve.

In the case of elliptic curves represented as plane cubics, the traditional definition of the group law implies that the image of a point of E_1 by the above correspondence must be a degree 3 divisor on E_2 equivalent to zero, so this divisor is defined by a line in $\mathbb{P}^2$ (a *secant* of E_2), which is a point in the dual projective plane $(\mathbb{P}^2)^\vee$. A natural candidate for the $\mathbb{P}^1$-bundle containing H is thus a bundle of lines in $\mathbb{P}^1$ defined by a map $E_1 \to (\mathbb{P}^2)^\vee$.

Moreover, since the map $H \to E_2$ has degree 3, we expect each point of E_2 to appear in 3 such lines, so the map $E_1 \to (\mathbb{P}^2)^\vee$ would have degree 3. Any such map is the composite of a group translation and a (linear) projective transformation, so a natural candidate to realise the triple cover is a diagram:

$$\begin{array}{ccccc} H & \hookrightarrow & \mathcal{L} & \hookrightarrow & \mathcal{Q} \\ \downarrow & & \downarrow & & \downarrow \\ E_1 \times E_2 & \hookrightarrow & E_1 \times \mathbb{P}^2 & \hookrightarrow & (\mathbb{P}^2)^\vee \times \mathbb{P}^2 \end{array}$$

where $\mathcal{L}$ is a bundle of lines (a $\mathbb{P}^1$-fibration over E_1) which is the pullback of the incidence variety $\mathcal{Q} = \{(\ell, P) \text{ such that } P \in \ell\} \subset (\mathbb{P}^2)^\vee \times \mathbb{P}^2$, seen as a tautological $\mathbb{P}^1$-bundle, by $E_1 \to (\mathbb{P}^2)^\vee$.

Then H could be viewed as the fiberwise intersection of $E_1 \times E_2$ with $\mathcal{L}$ which is a degree 3 cover of E_1.

The hyperelliptic involution $\iota : H \to H$ defines a rational quotient $H_\iota \simeq \mathbb{P}^1$ and commutes with the projection maps as in diagram:

$$\begin{array}{ccccc} E_1 \subset \mathbb{P}^2 & \xleftarrow{\pi_1} & H \subset E_1 \times E_2 & \xrightarrow{\pi_2} & E_2 \subset \mathbb{P}^2 \\ \downarrow{\scriptstyle x_1} & & \downarrow{\scriptstyle x_H} & & \downarrow{\scriptstyle x_2} \\ \mathbb{P}^1 & \xleftarrow[u_1]{} & \mathbb{P}^1 & \xrightarrow[u_2]{} & \mathbb{P}^1 \end{array}$$

All vertical arrows in the diagram are quotients by the hyperelliptic involution (x coordinate). In particular, H is stable under involution $(y_1, y_2) \to (-y_1, -y_2)$.

In particular, the rational functions u_1 and u_2 have degree 3, and the image of H in $\mathbb{P}^1 \times \mathbb{P}^1$ through (u_1, u_2) is a rational cubic of degree $(3, 3)$.

We will need the following property proved in [Kuh88].

Theorem 2.2. *Let $\{C_1, \dots, C_6\}$ be the 6 Weierstrass points of H. Then up to permutation, $\{C_1, C_2, C_3\}$ is the preimage of the zero point of E_1 and $\{C_4, C_5, C_6\}$ map to the 3 other Weierstrass points of E_1, and conversely for the projection $H \to E_2$.*

In particular, there exists an equation for $H : y^2 = P(x)Q(x)$ where P and Q have degree 3 such that the x-coordinates of the projection maps have denominator P and Q. This will be revisited with more detail in the next sections.

2.3. **The canonical duality of the projective plane.** In appropriate coordinates, the incidence variety

$$\mathcal{Q} = \{(P, \ell) \text{ such that } P \in \ell\} \subset \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$$

can be defined by a bilinear equation $x_1, x_2 + y_1 y_2 + z_1 z_2 = 0$. The quadratic form $x^2 + y^2 + z^2$ can be used to identify $\mathbb{P}^2$ with the dual plane and define a polarity relation where a point $P = [a : b : c]$ is associated to the line $\ell_P : ax + by + cz = 0$. Throughout this article ℓ_P will always denote the polar line of P w.r.t. that particular quadratic form.

For this duality relation, the polar of a flex point P_0 intersects Hesse cubics at the 3 Weierstrass points of the projection from pole P_0 (the polar line of $[1 : -1 : 0]$ is the line $\{x = y\}$), which conveniently coincides with the relation between Weierstrass points of H, E_1, E_2 described in [Kuh88].

We therefore define the curve:

$$\tilde{H} = \{x_1 x_2 + y_1 y_2 + z_1 z_2 = 0\} \subset E_1 \times E_2$$

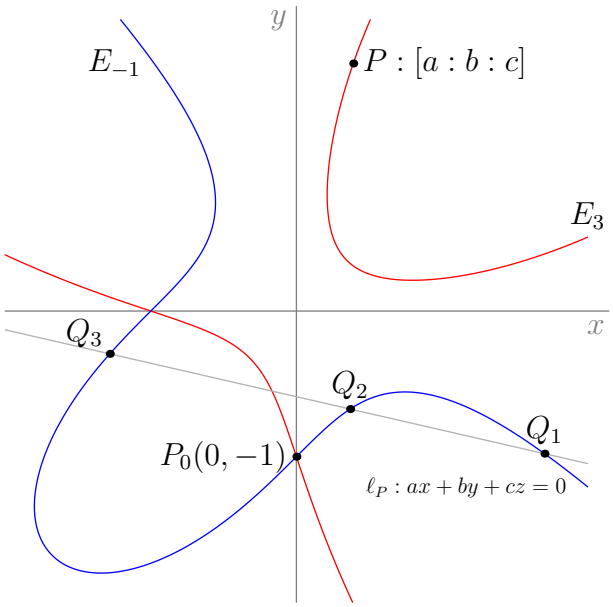


FIGURE 1. The polarity relation over $\mathbb{R}$, where $(P, Q_i) \in \tilde{H}$

This is a genus 10 curve with a free action of the group $\Gamma = (\mathbb{Z}/3\mathbb{Z})^2$ acting by translation on both E_1 and E_2 via its generators:

$$\gamma_1 : ([x_1 : y_1 : z_1], [x_2 : y_2 : z_2]) \mapsto ([z_1 : x_1 : y_1], [z_2 : x_2 : y_2])$$
$$\gamma_2 : ([x_1 : y_1 : z_1], [x_2 : y_2 : z_2]) \mapsto ([x_1 : jy_1 : j^2 z_1], [x_2 : j^2 y_2 : j z_2])$$

The inverted roots of unity on the second factor are reminiscent of Kani's property: a genus 2 triple cover is determined by an anti-isometry over the 3-torsion groups of E_1 and E_2.

The computation of genus can be done using the determination of ramification points (see below) and the Riemann-Hurwitz formula.

We will be interested in the quotient on this curve by Γ, which is a genus 2 curve.

2.4. **Tangents and ramification.**

Theorem 2.3. *Let (p_1, p_2) be a point of $\tilde{H}$. The differential of the map $\tilde{H} \to E_i$ can be identified with the linear equations of ℓ_{p_2} and ℓ_{p_1}.*

In particular, the projection to E_i is ramified if and only if the polar line through p_i is tangent to E_i.

Proof. This is a consequence of the equation of $\tilde{H}$. The differential of $x_1x_2+y_1y_2+z_1z_2$ is $(x_1, y_1, z_1)\cdot d(x_2, y_2, z_2)+(x_2, y_2, z_2)\cdot d(x_1, y_1, z_1)$ where symbol $\cdot$ is the "dot product" corresponding to the standard bilinear form.

In particular, the projection to E_2 is ramified if and only if the tangent space of E_2 is orthogonal to (x_1, y_1, z_1) for the standard bilinear form, which is the same equation as the polar line ℓ_1. □

This allows to determine the condition for the special triple covers in a geometric way (*special* in the sense of [Sha04] refers to triple covers having a single triple ramification point).

Lemma 2.4. *A triple cover is special (i.e. the map $H \to E_2$ has a triple ramification point) if and only if a Weierstrass point of E_1 is conjugate to a tangent through a flex point of E_2.*

The corresponding condition in terms of Hesse pencil parameters can be illustrated by the case of the flex point $[1 : -1 : 0]$. The tangent line of E_t at this point has coordinates: $[x^2 - tyz : y^2 - tzx : z^2 - txy] = [1 : 1 : t]$ which belongs to the pencil member E_μ for $\mu = (t^3 + 2)/(3t)$.

Moreover, since $[1 : 1 : t]$ lies on line $\{x = y\}$ it is a Weierstrass point on E_μ.

The curve E_μ is known as the Cayleyan curve of E_t and the construction of the genus 2 triple cover in that case can be found in [Kuw11].

2.5. **The singular case and isogenous elliptic curves.** From Kani's theorem [Kan97], the quotient $E_1 \times E_2/\Gamma$ fails to be a genus 2 Jacobian if and only if the isomorphism $E_1[3] \simeq E_2[3]$ is induced by an isogeny of degree 2.

A geometric construction of such isogenies is provided in [Dol12, Section 3.2.2] and can be summarised by the following property (relating the Hessian curve and the Cayleyan curve of a given cubic):

Proposition 2.5. *Let E_t be a Hessian cubic curve, and let τ be an involution corresponding to translation by a 2-torsion point.*

Then the set of lines $(P, \tau(P))$ is also a Hessian cubic curve E_u in the dual projective plane, and the map $f : P \to (P, \tau(P)) \in (\mathbb{P}^2)^\vee$ is a degree 2 isogeny.

By definition, a line in the dual projective plane can be identified with its polar point in $\mathbb{P}^2$. So for every point $P \in E_t$, P and $\tau(P)$ are conjugates to $f(P) \in E_u$.

If $\tilde{H}$ is the triple cover of E_t and E_u defined by the polarity relation, the latter property implies the existence of a section $E_t \to \tilde{H}$ by $P \mapsto (P, f(P))$, which would be impossible if $\tilde{H}$ was a smooth curve of genus $g > 1$.

Proposition 2.6. *Let $\phi : E_\lambda \to E_\mu$ be a degree 2 isogeny between curves in Hesse form, and let $\tilde{H}$ be the set of conjugate points in $E_\lambda \times E_\mu$ using the above construction.*

Then $\tilde{H}$ is not irreducible and is the union of the graph of ϕ and the (translated) graph of the dual isogeny.

Proof. From the dual construction above, we can identify ϕ with the map $P \mapsto \ell(P, P + \epsilon)$ where ϵ is the order 2 point in the kernel of ϕ.

According to the secant group law, since $\phi(P) = \phi(P + \epsilon) = Q$, the polar line ℓ_Q goes through P, $P + \epsilon$ and $-2P - \epsilon$.

This means that $\tilde{H}$ consists of pairs $(P,Q) = (P,\phi(P))$, $(P+\epsilon,Q) = (P+\epsilon,\phi(P+\epsilon))$ (belonging to the graph of ϕ) and $(-2P-\epsilon,Q) = (-\phi^*(Q)-\epsilon,Q)$ (belonging to the translated graph of the dual isogeny ϕ^*).

In particular, $\tilde{H}$ is the union of 2 irreducible components isomorphic to E_λ and E_μ.

These irreducible components meet when $Q = \phi(-\phi^*(Q)-\epsilon) = -2Q$, that is, exactly along the graph of ϕ restricted to the 3-torsion subgroup. □

This decomposition corresponds to the classically known fact that a Theta divisor on a principally polarised abelian variety is reducible when the abelian variety decomposes as a product. The union of 2 elliptic curves intersecting at 9 points has arithmetic genus equal to 10, which is the same as the smooth case.

3. Geometry of the genus 2 triple cover

This section establishes several properties that will be used for explicit computations in 4.

The action of group Γ on $\mathbb{P}^2$ is generated by projective transformations:

$$[x:y:z] \mapsto [y:z:x]$$

$$[x:y:z] \mapsto [x:\alpha y:\alpha^2 z] \text{ for } \alpha \in \mu_3$$

This action has no fixed point on each smooth member E_t of the Hesse pencil.

Across this section we will use Halphen's coordinates defining a degree 9 rational map $\mathbb{P}^2 \to \mathbb{P}^2$. This map is invariant under Γ and acts on each element of the Hesse pencil as the isogeny $[3] : P \mapsto 3P$, so the tripling map [3] realises a quotient $\mathbb{P}^2 \to \mathbb{P}^2/\Gamma$.

The Halphen coordinates correspond to the fact that the formula for computing the triple of a point for the elliptic curve group law, choosing a given flex point as origin (we have chosen $[1:-1:0]$) are independent of the parameter t and defined by universal polynomials:

$$X = x^6y^3 + y^6z^3 + z^6x^3 - 3x^3y^3z^3$$
$$Y = x^3y^6 + y^3z^6 + z^3x^6 - 3x^3y^3z^3$$
$$Z = xyz(x^6 + y^6 + z^6 - x^3y^3 - y^3z^3 - z^3x^3)$$

3.1. **The genus 2 triple cover as a quotient correspondence.** We have established that the polarity conjugacy relation defines a Γ-equivariant degree 3 correspondence between a pair of elliptic curves in Hesse normal form.

As a consequence the quotient $\tilde{H} \to H = \tilde{H}/\Gamma$ is an unramified map with genus 2 ($2g_H - 2 = (2g_{\tilde{H}} - 2)/9 = 2$ and the following diagram commutes:

$$\begin{array}{ccccc} E_1 & \longleftarrow & \tilde{H} & \longrightarrow & E_2 \\ {\scriptstyle [3]}\downarrow & & \downarrow{\scriptstyle /\Gamma} & & \downarrow{\scriptstyle [3]} \\ E_1 & \longleftarrow & H & \longrightarrow & E_2 \end{array}$$

The projections from H to E_i have degree 3. By Riemann-Hurwitz formula, the map $H \to E_i$ has 2 ramification points which are exchanged by the hyperelliptic involution (or in the *special case*, a triple ramification point which is a Weierstrass point) [Kuh88].

Theorem 3.1. *The embedding*

$$H \simeq \tilde{H}/\Gamma \hookrightarrow (E_1 \times E_2)/\Gamma$$

is isomorphic to the embedding of H as a Theta divisor in its Jacobian.

In particular $E_1 \times E_2 \to \operatorname{Jac} H$ *is a* $(3,3)$*-isogeny with kernel*

$$\Gamma \simeq \{(T_1, T_2) \in E_1[3] \times E_2[3] \text{ such that } T_1 = T_2 \text{ in } \mathbb{P}^2\}$$

It should be noted that whereas $\tilde{H}$ is embedded as a smooth curve in $E_1 \times E_2$, the projection maps from H to E_i do not define a smooth embedding $H \subset E_1 \times E_2$. The map $H \to E_1 \times E_2$ factors through $(E_1 \times E_2)/\Gamma \to E_1 \times E_2$ and the final image of H has singularities. The following sections will show that it generically has 8 double points, which is consistent with the fact that a bilinear pairing generates a polarity correspondence which is represented by a curve of arithmetic genus 10.

3.2. **The polarity relation on quotient H.** Using the same properties as the first section, we can determine that the following property is true:

Proposition 3.2. *The degree 3 correspondence* $E_1 \leftarrow H \to E_2$ *defines a map* $E_1 \to (\mathbb{P}^2)^\vee$ *which is induced by a projective transformation or equivalently by polarity via a bilinear pairing.*

This bilinear pairing b_{t_1,t_2} *depends on the Hesse parameters* t_1 *and* t_2 *and is not always symmetric.*

Embeddings of an elliptic curve in a projective plane can differ by translations by an elliptic curve element and by projective transformations.

Here the fact that the zero element is mapped to the secant through the 3 associated Weierstrass points (which have a zero sum) is in favour of looking for a purely projective transform.

We prove this proposition by constructively building the matrix. The coefficients can be obtained through formal computation (see section 4.3). They were determined by interpolating rational functions through numerical simulations (over finite fields) and checking that the composite equation $b_{t_1,t_2}(3P_1, 3P_2) = 0$ on $E_1 \times E_2$ (a bilinear combination of Halphen coordinates) belongs to the ideal defining $\tilde{H}$.

To avoid confusion when referring to the polarity relation defined by bilinear form b_{t_1,t_2} the notation ℓ^1_P will be used (and ℓ^2_Q for the polar line w.r.t. bilinear form b_{t_2,t_1}).

3.3. **Projection to $\mathbb{P}^1 \times \mathbb{P}^1$.** Since 2-torsion points are sent to themselves by the tripling map [3], in the quotient representation the distinguished origin $[1:-1:0]$ is still conjugate to the line $\{x = y\}$ through the 3 Weierstrass points of either E_1 or E_2, even when considering the parametre-dependent bilinear relation b_{t_1,t_2}.

Since the tangent line at origin has dual coordinates $[1:1:t]$, we can define the projection from the origin with formula $z/(x+y+zt)$, which is invariant by the involution $[x:y:z] \mapsto [y:x:z]$ and maps E_i to $\mathbb{P}^1$ (the origin is mapped to the infinity point).

The 2 projections to $\mathbb{P}^1$ define a rational (hence regular) map from H to $\mathbb{P}^1 \times \mathbb{P}^1$ via $E_1 \times E_2$. The 2 triples of Weierstrass points of E_1 and E_2 are mapped to the 2 lines at infinity in $\mathbb{P}^1 \times \mathbb{P}^1$.

Since this projection realises the quotient by the hyperelliptic involution of H, we expect the image of H to be a rational curve. Additionally, the "horizontal" and "vertical" pencils of lines lift to pencils of lines through the origin $P_0 = [1:-1:0]$ in $\mathbb{P}^2$. Each such line generically meets E_1 (or E_2) in 2 points outside P_0, thus defines 6 points in H (3 pairs of points exchanged by the hyperelliptic involution). This implies that the image of H in $\mathbb{P}^1 \times \mathbb{P}^1$ is expected to have degree (3,3).

A degree $(3,3)$ in $\mathbb{P}^1 \times \mathbb{P}^1$ has generic genus 4 ($2g_a - 2 = C \cdot (C + K_{\mathbb{P}^1 \times \mathbb{P}^1}) = (3,3) \cdot (1,1) = 6$). Since the image of H is a rational curve, we expect it to have 4 singular points, corresponding to generically 8 singular points in $E_1 \times E_2$.

Each point of $\mathbb{P}^1 \times \mathbb{P}^1$ defines a birational map to $\mathbb{P}^2$ by blowing up that point and contracting the horizontal and vertical lines through it ($L^2 = (L+E)^2 - 2L \cdot E - E^2 =$

-1). Choosing the point at infinity (∞, ∞) recovers the birational map $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ which coincides with the identity map on the open set corresponding to the affine plane $\mathbb{A}^2$.

Thus if the 4 singular points are in general position, a standard quadratic transformation centered at one of these points, followed by a quadratic transformation based on the triangle formed by the 3 other points, will resolve all singularities and establish a birational map from H_ι to a conic (we will see that the scenario of a triple point is also possible). This process is detailed in section 4.7.

The singular case. When $\tilde{H}$ becomes reducible as the union of the graph of a 2-isogeny $\phi : E_1 \to E_2$ and its dual (see section 2.5) the graph of ϕ has degrees $(1, 2)$ with respect to the projections, and the graph of ϕ^* has degree $(2, 1)$. These graphs are invariant by action of Γ so the final image of $\tilde{H}$ in $\mathbb{P}^1 \times \mathbb{P}^1$ is a union of conics of degrees $(1, 2)$ and $(2, 1)$ intersecting in 4 points. This can be detected in the implementation by obtaining a degree 2 instead of 6 in the rational parameterisation.

3.4. **Twisted dual curves and double points.** A specific situation arises when $\tilde{H}$ contains pairs (P, Q) and (P, Q') such that $3Q = 3Q'$ (meaning that Q and Q' differ by a 3-torsion element). In that case, the corresponding points of H map to the same pair $(3P, 3Q)$ in $E_1 \times E_2$.

In other words, while ℓ_P is a secant of E_2, the line ℓ^1_{3P} is tangent to E_2 at $3Q$. By Γ invariance, we observe that if $\tilde{H}$ contains (P, Q) and $(P, Q + T)$, it also contains $(P - T, Q)$ thus the polar line ℓ^2_{3Q} is tangent to E_1 at point $3P$.

Lemma 3.3. *The locus of lines $(Q, Q+T)$ defines a singular sextic E_2^T in the dual projective plane. When identified to a sextic in $\mathbb{P}^2$ via the $x^2 + y^2 + z^2$ duality, it intersects E_1 in 18 points forming 2 Γ-orbits exchanged by the canonical involution.*

Explicit equations for these *twisted* dual curves will be given in the last section. Since E_2^T and E_2^{-T} have the same definition, we can define 4 such twisted duals.

Since pairs (P, Q) and $(P, Q + T)$ are *not* in the same orbit for the action of Γ, they do not define the same point of H, even though they map to the same point $(3P, 3Q) \in E_1 \times E_2$.

It results that each twisted dual curve defines a double point of the image of H in $\mathbb{P}^1 \times \mathbb{P}^1$. The coordinates of these double points are given by rational functions of t_1 and t_2 and are computed in section 4.

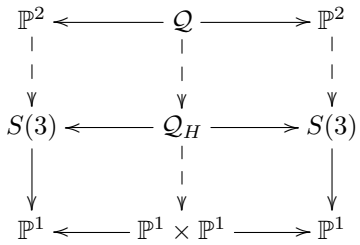
The case of triple points. Under adequate conditions, it may happen that a line ℓ_P contains Q, $Q + T_1$ and $Q + T_2$ where T_2 and T_1 are linearly independent (the case $T_2 = -T_1$ implies that Q is a 3-torsion point, which has already been studied). In this situation Q is necessarily a 9-torsion point.

This means that P belongs to the 3 twisted duals $E_2^{T_1}$, $E_2^{T_2}$ and $E_2^{T_1 - T_2}$, and any point belonging to 2 twisted duals automatically belongs to the third one.

Similarly, the points (P, Q), $(P, Q + T_1)$, $(P, Q + T_2)$ do not define the samme Γ-orbit and are 3 different points of H mapping to the same point $(3P, 3Q)$ in $E_1 \times E_2$. This situation defines a triple point in the image of H in $E_1 \times E_2$.

This triple point will also be visible in the image in $\mathbb{P}^1 \times \mathbb{P}^1$.

3.5. **A family of genus 2 coverings.** Since the Hesse pencil is isomorphic to the universal family of elliptic curves with a 3-level structure, the family:



where $\mathcal{Q}$ is the quadric defined by the polarity relation and the downward arrow are quotients under the action of Γ, and $S(3)$ is the blow-up of $\mathbb{P}^2$ along the 9 base points of the Hesse pencil, define a universal family of triple coverings of elliptic curves by a genus 2 curve (for any pair of elliptic curve with a choice of symplectic 3-torsion basis, the genus 2 triple cover is known to be unique up to isomorphism).

Over the open locus of $\mathbb{P}^1 \times \mathbb{P}^1$ corresponding to pairs of smooth elliptic curves ($t \neq \infty$ and $t^3 \neq 1$), each fibre is either a smooth genus 2 curve, or a stable curve isomorphic to the two elliptic curves joined by the origin $E_1 \sqcup E_2$.

Further properties of this family as an actual scheme-theoretic moduli space (in particular as representing a sheaf in an appropriate topology) are not in scope of this work.

In particular, the existence of this family does not imply that it is globally isomorphic to a family of hyperelliptic curves defined by equations $y^2 = H(x)$, even if it is true pointwise.

4. Computing explicit equations of the triple cover

A base field of definition $\Bbbk$ is fixed for these computation, in order to distinguish cases where the geometric situation (over $\bar{\Bbbk}$) can differ from the base field situation.

Most explicit equations in this section were obtained using software SageMath [SAGE] and Singular [DGPS22] by writing equations on $\tilde{H}$ and descending to the quotient in Halphen coordinates $[X : Y : Z]$ by variable elimination.

In several cases the following systems of intermediate coordinates were found to be useful (assuming $[x : y : z] \in E_t$):

$$\begin{aligned} u &= xyz & u &= xyz \\ v &= x^6y^3 + y^6z^3 + z^6x^3 & v &= x^2y + y^2z + z^2x \\ w &= x^3y^6 + y^3z^6 + z^3x^6 & w &= xy^2 + yz^2 + zx^2 \\ X &= v - 3u^3 & X &= v^3 - 3uvw \\ Y &= w - 3u^3 & Y &= w^3 - 3uvw \\ tZ &= 9(t^3-1)u^3 - v - w & Z &= 3(t+1)uvw - v^3 - w^3 \\ & & Z &= 9(t^2+t+1)u^3 - 3uvw \end{aligned}$$

Polynomials with Γ-invariance are often easier to write as functions of u, v, w, lowering their degree before performing elimination to use Halphen coordinates.

4.1. **Coordinates of the pair of ramification points.** A projection $\tilde{H} \to E_2$ is ramified over a point p iff the polar line (with respect to the standard bilinear form) ℓ_p is tangent to E_2 (see section 2.4). The set of ramification points is invariant under the hyperelliptic involution and the action of Γ, and can be expressed as the intersection of E_1 and the dual variety $E_2^\vee$ which is the locus of tangent lines to E_2, viewed in $(\mathbb{P}^2)^\vee \simeq \mathbb{P}^2$.

The dual curve can be represented by a (singular) plane sextic and its equation can be found in [AD09] or [Dol12, Section 3.2.3]:

$$\begin{aligned}
&E_1 : x^3 + y^3 + z^3 = 3t_1xyz\\
&E_2 : x^3 + y^3 + z^3 = 3t_2xyz\\
&E_2^\vee : x^6 + y^6 + z^6 + (4t_2^3 - 2)(x^3y^3 + y^3z^3 + z^3x^3)\\
&- 6t_2^2xyz(x^3 + y^3 + z^3) + (12t_2 - 3t_2^4)x^2y^2z^2 = 0
\end{aligned}$$

Using intermediate coordinates

$$\begin{aligned}
u &= xyz\\
v &= x^6y^3 + y^6z^3 + z^6x^3\\
z &= x^3y^6 + y^3z^6 + z^3x^6
\end{aligned}$$

we can find a low-degree member of the ideal of $E_1 \cap E_2^\vee$ using a computer-assisted computation:

$$u^3(144t_1t_2^4 + 216t_1^2t_2^2 - 27t_1^3 - 96t_2^3 - 72t_1t_2 + 12) + (4 - 32t_2^3)(v + w) = 0$$

to obtain a linear equation in the quotient plane:

$$\begin{aligned}
&\tau = t_2^4 + 6t_1t_2^2 + t_1^2 - 4t_2\\
&(X + Y)(4t_1^2t_2^3 - \tau) = Z(\tau t_1 - 4t_1^3 + 4 - 4t_2^3)
\end{aligned}$$

for the ramification of $H \to E_2$.

This line goes through the distinguished origin $[1 : -1 : 0]$ of E_1 and cuts E_1 in 2 points exchanged by the hyperelliptic involution $X \leftrightarrow Y$.

By symmetry, exchanging t_1 and t_2 provides an explicit equation for the line through the origin intersecting E_2 at the ramification locus of $H \to E_1$.

In general, this relation is not symmetric (the image of H in $\mathbb{P}^1 \times \mathbb{P}^1$ cannot have a regular point such that both projections ramify at that point).

4.2. **Coordinates of double points.** The double points of the rational sextic in $\mathbb{P}^1 \times \mathbb{P}^1$ are the images of the intersection of E_1 with the *twisted* duals of E_2 defined in section 3.4.

For $\gamma \in \Gamma/\pm 1$ the twisted dual E_2^γ is the curve in the dual projective plane whose points are lines $(P, P + \gamma)$ for $P \in E_2$.

By symmetry, $E_2^\gamma = E_2^{-\gamma}$.

The equations of the twisted duals can be computed by variable elimination:

$$\begin{aligned}
E_2^{\gamma_0} :\quad & (xy)^3 + (yz)^3 + (zx)^3 - 3t(x^2y^2z^2) = 0\\
E_2^{\gamma_1} :\quad & x^6 + y^6 + z^6 + (3jt - 1)(x^3y^3 + y^3z^3 + z^3x^3)\\
& - 3j(jt + 1)(x^4yz + y4zx + z^4yx) + (3jxyz)^2 = 0\\
E_2^{\gamma_2} :\quad & x^6 + y^6 + z^6 + (3j^2t - 1)(x^3y^3 + y^3z^3 + z^3x^3)\\
& - 3j^2(j^2t + 1)(x^4yz + y^4zx + z4yx) + (3j^2xyz)^2 = 0\\
E_2^{\gamma_3} :\quad & x^6 + y^6 + z^6 + (3t - 1)(x^3y^3 + y^3z^3 + z^3x^3)\\
& - 3(t + 1)(x^4yz + y^4zx + z^4yx) + (3xyz)^2 = 0
\end{aligned}$$

where $\gamma_0 : [x : y : z] \mapsto [x : jy : j^2z]$, $\gamma_1 : [x : y : z] \mapsto [z : jx : j^2y]$, $\gamma_2 : [x : y : z] \mapsto [z : j^2x : jy]$, $\gamma_3 : [x : y : z] \mapsto [z : x : y]$.

The pairs of special points above double points are located on lines:

$$\begin{aligned}
L_0 &: (x+y)(t_1^2 - t_2) - z(t_1t_2 - 1) = 0\\
L_1 &: (x+y)(jt_1t_2 - j) + z(t1^2 - j^2t_1t_2 - t_2 + j^2) = 0\\
L_2 &: (x+y)(j^2t_1t_2 - j^2) + z(t_1^2 - jt_1t_2 - t_2 + j) = 0\\
L_3 &: (x+y)(t_1t_2 - 1) + z(t_1^2 - t_1t_2 - t_2 + 1) = 0
\end{aligned}$$

The equation of $E_2^{\gamma_0}$ makes it clear that it is the image of E_2 by the standard quadratic birational transformation $[x : y : z] \mapsto [yz : zx : xy]$ based on an inflection triangle (3 lines going through all 9 inflection points). There are 4 such triangles in the Hesse configuration.

The equations above are defined over the base field $\Bbbk$ and define $\Bbbk$-rational points in $\mathbb{P}^1 \times \mathbb{P}^1$. However it is not true in general that the branches at these singular points are themselves defined over $\Bbbk$.

4.3. **Determination of the polar transformation.** The polynomial coefficients of the polarity relation defining H as a correspondence in $E_1 \times E_2$ were determined by numerical simulations using the following process:

(1) choose a base field with large enough characteristic (e.g. $\mathbb{F}_{65537}$);
(2) generate random Hesse equation parametres;
(3) for each (t_1, t_2) determine orthogonal pairs $P \in E_1$ and its polar line ℓ_P intersecting E_2 at 3 rational points, and their image via the [3] tripling morphism;
(4) once 4 projectively independent pairs $(3P, \ell_{3P})$ are obtained, compute the unique transformation matrix $M(t_1, t_2)$ realising this polarity relation.

It turns out that the coefficients of M have degree ≤ 4 in each variable t_1 and t_2 so the system can be overdetermined by generating enough relations.

Once candidate polynomials are found, it can be further confirmed by running the same process on a larger field (for example $\mathbb{F}_{2^{32}-5}$) and verifying the result formally by checking that the resulting equation $b_{t_1,t_2}(3P_1, 3P_2) = 0$ lifts to a function on $\mathbb{P}^2 \times \mathbb{P}^2$ belonging to the ideal of $\tilde{H}$ (generated by the equations of E_1, E_2 and the standard bilinear form). The final verification can be done on field $\mathbb{Q}(t_1, t_2)$.

The transformation matrix (which is the matrix of bilinear form b_{t_1,t_2}) can be computed explicitly:

$$M = \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{01} & m_{00} & m_{02} \\ m_{20} & m_{20} & m_{22} \end{pmatrix}$$

$$\begin{aligned}
m_{00} &= 3t_1^3t_2^3 - 3t_1^2t_2^2 - 2t_1^3 - 2t_2^3 + 3t_1t_2 + 1\\
m_{01} &= t_1^3 + t_2^3 - 3t_1^2t_2^2 + 3t_1t_2 - 2\\
m_{02} &= t_1^4 - 3t_1^3t_2^2 + 3t_1^2t_2 + t_1t_2^3 - 2t_1\\
m_{20} &= t_2^4 - 3t_1^2t_2^3 + 3t_1t_2^2 + t_1^3t_2 - 2t_2\\
m_{22} &= t_1^4t_2 + t_1t_2^4 + 3t_1^2t_2^2 - 3t_1^3 - 3t_2^3 - 2t_1t_2 + 3\\
\det M &= (t_1^3 - 1)^2(t_2^3 - 1)^2(t_1t_2 - 1)\\
&\quad \times (t_1 + t_2 + 1)(t_1 + j^2t_2 + j)(t_1 + jt_2 + j^2) \text{ where } j^3 = 1
\end{aligned}$$

The coefficients were obtained by running numerical computations on a small finite field, interpolating using rational functions of lowest degree, with a final formal verification over $\mathbb{Z}[j]$.

4.4. **Equation of the rational sextic.** The image H_ι of H in $\mathbb{P}^1 \times \mathbb{P}^1$ can be determined by variable elimination, but the previous properties provide enough constraints to determine entirely its equation.

Lemma 4.1. *Let $[u : u'], [v : v']$ be projective coordinates so that $u/u' = z_1/(x_1 + y_1 + t_1 z_1)$ and $v/v' = z_2/(x_2 + y_2 + t_2 z_2)$ are affine coordinates for E_1/ι and E_2/ι.*

Then the specialisation of H_ι to $u' = 0$ is the cubic polynomial for the normalised $y^2 = C_2(x)$ equation of E_2, and the specialisation of H_ι to $v' = 0$ is the cubic polynomial for the normalised equation of E_1 ($y^2 = C_1(x)$).

Proof. This follows directly from the fact that H contains the pairs $(O_1, W_{2,i})$ and $(W_{1,i}, O_2)$ for $i = 1, 2, 3$. □

The conventions chosen earlier imply that the basis of the 3-torsion is sent to coordinates $1/(t-1)$ and 0 respectively (the other 3-torsion points will have coordinates $j/(jt-1)$ and $j^2/(j^2t-1)$) which defines uniquely the normalised equation of E_i.

In addition to that, the first coordinate of double points has been computed earlier, so a linear relation $(x + y)A + zB = 0$ gives $u = A/(t_1 A - B)$:

$$D_{0,u} = \frac{t_1^2 - t_2}{t_1^3 - 1}$$
$$D_{1,u} = \frac{jt_1t_2 - j}{jt_1(t_1t_2 - 1) - (t_1^2 - j^2t_1t_2 - t_2 + j^2)}$$
$$D_{2,u} = \frac{j^2(t_1t_2 - 1)}{j^2t_1(t_1t_2 - 1) - (t_1^2 - jt_1t_2 - t_2 + j)}$$
$$D_{3,u} = \frac{t_1t_2 - 1}{t_1(t_1t_2 - 1) - (t_1^2 - t_1t_2 - t_2 + 1)}$$

The coordinate v is obtained by exchanging t_1 and t_2 in formulas.

Theorem 4.2. *Assuming the equation of H_ι is normalised as*

$$\begin{aligned} &u^3v^3 + v^3(a_{2,1}u^2u' + a_{4,1}uu'^2 + a_{6,1}u'^3) \\ &+ u^3(a_{2,2}v^2v' + a_{4,2}vv'^2 + a_{6,2}v'^3) \\ &+ u'v'F(u, u', v, v') \end{aligned}$$

where F is a homogeneous polynomial of degree (2, 2). The nine coefficients of F are entirely determined by the constraint of having double points $(D_i)_{i=0,1,2,3}$, or a triple point D_0 and a double point D_1.

Each double point defines 3 constraints by the vanishing of the equation polynomial and its first order derivatives. A triple point defines 6 constraints, with the additional vanishing of second order derivatives.

4.5. **Rational parameters for the rational sextic.** The quotient of H by the hyperelliptic involution (H_ι) defines a correspondence between the x coordinates of E_1 and E_2, represented by Weierstrass equations by the choice of the origin point.

As described earlier, its singularities can be resolved by a sequence of linear transformations and quadratic birational transformations to a plane conic, which is parameterised by rational functions by projection from any rational point.

The distinguished rational point can be a known regular point (the ramification point, a rational Weierstrass point) or a branch of one of the double points if its tangent line is known.

In the triple point case, the first quadratic transformation can resolve the triple point and leave only one node: the result is then a nodal plane cubic, which readily admits a rational parameterisation.

In the singular case, the sextic equation defines a reducible curve which is a union of conics and this calculation will return rational functions of degree 1 and 2.

4.6. **Hyperelliptic equation of H.** The previous calculations allow to fully determine equations for the morphisms $H/\iota \to E_i/\iota$ between rational curves (the x coordinates) but the lift to a double cover is possibly only defined up to a quadratic twist. However, the existence of rational points will allow to resolve these indeterminacies.

Lemma 4.3. *If the base field $\Bbbk$ is finite, H has at least one non-Weierstrass rational point $(e_1, e_2) \times E_1 \times E_2$.*

Proof. Since $\operatorname{Jac} H$ is isogenous to $E_1 \times E_2$, the action of Frobenius on its étale cohomology group is entirely determined by E_1 and E_2, implying that the order of H is $q + 1 - \operatorname{Tr}(E_1) - \operatorname{Tr}(E_2) > q - 4\sqrt{q}$ (see also [BHLS15] for an explanation). For $q \geq 29$ this is larger than 7.

As we assume existence of cubic roots of unity and characteristic different from 2 and 3, the only remaining values of q are 7, 13 and 19. When $q = 7$ the only possible trace for E_i is -1 (so that the order of E_i is 9), giving $\#H(\mathbb{F}_7) = 10$. When $q = 19$ the traces can be 2 or -7 (elliptic curve order 18 or 27) so $\#H(\mathbb{F}_{19}) \geq 16$.

When $q = 13$ the traces can be -5 and 4 so it may happen that $\#H(\mathbb{F}_{13}) \geq 6$. The existence of a non-Weierstrass rational point in that case can be determined by explicit computation and enumeration of field elements. □

Assuming the same conventions as before, we have determined explicit rational functions of degree 3:

$$T \mapsto \left(\frac{\mathrm{NX}_1(T)}{\mathrm{DX}_1(T)}, \frac{\mathrm{NX}_2(T)}{\mathrm{DX}_2(T)}\right) \in H_\iota \subset \mathbb{P}^1 \times \mathbb{P}^1$$

realising a birational map from $\mathbb{P}^1$ to H_ι. We can normalise polynomials by requiring that DX_1 and DX_2 are monic, degree 3 polynomials.

Since the Weierstrass points of E_1 and E_2 lie on the two lines at infinity, $\mathrm{NX}_2 \,/\, \mathrm{DX}_2$ maps the roots of DX_1 to the coordinates of the Weierstrass points of E_2, and conversely. These 6 points of H_ι are known to be the Weierstrass points of H [Kuh88].

Following equations given in [Kuh88, BHLS15], we are looking for an equation $y_H^2 = \alpha \,\mathrm{DX}_1(x_H)\,\mathrm{DX}_2(x_H)$ for some scalar constant α where x_H is identified with the rational parameter T.

We also assume that E_1 and E_2 have been reduced, using affine transformations, to the standard Weierstrass equation defined by affine coordinates $u = z/(x+y+tz)$ and $v = (x-y)/(x+y+tz)$ for a Hessian curve, which is:

$$3v^2 = 4(t^3 - 1)u^3 - 9t^2u^2 + 6tu - 1$$

Lemma 4.4. *The polynomial $P_1(\mathrm{NX}_1 \,/\, \mathrm{DX}_1)\,\mathrm{DX}_1^3$ is a multiple of DX_2 and the quotient by DX_2 admits a square root as a polynomial R_1 up to a multiplicative constant.*

Proof. Through the rational parametrisation $\mathbb{P}^1 \to H_\iota$ we can geometrically interpret the corresponding divisors.

The polynomial DX_2 defines a divisor which is the intersection with line at infinity $\mathbb{P}^1 \times \{\infty\}$, corresponding to Weierstrass points of E_1.

The zeros of $P_1(\mathrm{NX}_1 \,/\, \mathrm{DX}_1)$ correspond to the T-coordinates of Weierstrass points of E_1, so $P_1(\mathrm{NX}_1 \,/\, \mathrm{DX}_1)\,\mathrm{DX}_1^3$ is a degree 9 effective divisor on $\mathbb{P}^1$ containing $\operatorname{div} \mathrm{DX}_2$.

The complement consists of 3 pairs of points which are the other preimages of the Weierstrass points of E_1 in H_ι, and since they are exchanged by the action of ι, they map to a point of multiplicity 2 (H_ι is tangent to the line $\{x = x(W_{1,i})\}$), implying that this divisor has a square root. □

Note that since

$$(x^3 + ax^2 + bx + c)^2 = x^6 + 2ax^5 + (2b + a^2)x^4 + (2c + 2ab)x^3 + \dots$$

the square root of a monic degree 6 polynomial can be computed using only elementary field operations. We can choose the multiplicative constant to be the leading coefficient of $P_1(\mathrm{NX}_1 / \mathrm{DX}_1)\,\mathrm{DX}_1^3$ which is $\alpha_1 = P_1(\mathrm{NX}_1(\infty)/\,\mathrm{DX}_1(\infty))$.

Since $P_1(\mathrm{NX}_1 / \mathrm{DX}_1)\,\mathrm{DX}_1^3 = \alpha_1\,\mathrm{DX}_2\,R_1^2$, this allows to define a map:

$$(x_H, y_H) \mapsto \Big(\frac{\mathrm{NX}_1(x_H)}{\mathrm{DX}_1(x_H)}, y_H \frac{R_1(x_H)}{\mathrm{DX}_1(x_H)^2}\Big)$$

satisfying the relation:

$$\Big(y_H \frac{R_1(x_H)}{\mathrm{DX}_1(x_H)^2}\Big)^2 = \alpha\,\mathrm{DX}_1(x_H)\,\mathrm{DX}_2(x_H)\frac{R_1(x_H)^2}{\mathrm{DX}_1(x_H)^4} = (\alpha/\alpha_1)P_1\Big(\frac{\mathrm{NX}_1(x_H)}{\mathrm{DX}_1(x_H)}\Big)$$

Let $(e_1, e_2) \in E_1 \times E_2$ be the image of a $\Bbbk$-rational point of H which is not a Weierstrass point of H ($y(e_1) \neq 0$ and $y(e_2) \neq 0$). If $\Bbbk$ is a finite field, this point is guaranteed to exist. Then $(x(e_1), x(e_2)) \in \mathbb{P}^1 \times \mathbb{P}^1$ is represented by a value of parameter $T \in \mathbb{P}^1(\Bbbk)$ and the following identities hold:

$$\alpha_1\,\mathrm{DX}_1(T)\,\mathrm{DX}_2(T)\frac{R_1(T)^2}{\mathrm{DX}_1(T)^4} = P_1(\mathrm{NX}_1(T)/\,\mathrm{DX}_1(T)) = y(e_1)^2$$

$$\alpha_2\,\mathrm{DX}_2(T)\,\mathrm{DX}_1(T)\frac{R_2(T)^2}{\mathrm{DX}_2(T)^4} = P_2(\mathrm{NX}_2(T)/\,\mathrm{DX}_2(T)) = y(e_2)^2$$

meaning that $\alpha_1\alpha_2$ is a square:

$$\alpha_1\alpha_2 = \left(\frac{y(e_1)y(e_2)\,\mathrm{DX}_1(T)\,\mathrm{DX}_2(T)}{R_1(T)R_2(T)}\right)^2$$

As a consequence, we can define the following final equations:

$$H : y^2 = \alpha_1\,\mathrm{DX}_1(x)\,\mathrm{DX}_2(x)$$
$$H \to E_1 : (x, y) \mapsto \left(\frac{\mathrm{NX}_1(x)}{\mathrm{DX}_1(x)}, y\frac{R_1(x)}{\mathrm{DX}_1(x)^2}\right)$$
$$H \to E_2 : (x, y) \mapsto \left(\frac{\mathrm{NX}_2(x)}{\mathrm{DX}_2(x)}, \frac{\alpha_2}{\sqrt{\alpha_1\alpha_2}}y\frac{R_2(x)}{\mathrm{DX}_2(x)^2}\right)$$

4.7. **An algorithm to compute the triple cover from elliptic curves with level structure.** In the above calculations, we can observe that if the input elliptic curves are given in Weierstrass form, the formulas depend on the Hesse pencil parameters t_1 and t_2 but the actual triple cover can be given in hyperelliptic form using solely the parameterisation of the sextic in $\mathbb{P}^1 \times \mathbb{P}^1$. The sextic is entirely determined by the location of the double points and computations can be done without referring to the Hessian equations nor to the polarity relations.

The algorithm can be summarised with the following steps:

(1) Compute Hesse pencil parameters from input data.
(2) Compute singularities of $H_\iota \subset \mathbb{P}^1 \times \mathbb{P}^1$ using explicit formulas.
(3) Compute the sextic model of H_ι from an overdetermined linear system.
(4) Compute a resolution of singularities as a chain of 2 quadratic transformations and deduce a rational parameterisation.
(5) Deduce full projection maps from the x-coordinate projections.

The algorithm only involves basic field operations and possible extraction of square roots needed for the following steps:

- A square of $\alpha_1\alpha_2$ is required to compute the final morphism. Additional input data of a non-Weierstrass rational point of H given by its images in $E_1 \times E_2$ can be used to compute a square root directly, arranging for the parameterisation to make $T = \infty$ correspond to the chosen point.
- Find a rational point on a conic requires heuristically a constant number (on average) of square roots. Additional input data of a regular rational point of H_ι, for example via a Weierstrass point of E_i (which defines a Weierstrass point of H) is enough to avoid that step.

Note that all steps up to (and including) the resolution of singularities can also be performed on field $\mathbb{Q}(t_1, t_2)$.

The author does not make any claim about the compared efficiency of this algorithm w.r.t. other known methods such as [BHLS15]. The operations are described as pseudocode here but a complete SageMath implementation is given as appendix.

Step 1. Compute Hesse parameter and associated Weierstrass form. We mentioned earlier that in normalised Weierstrass form, the basis of 3-torsion must be sent to $u(T_1) = -1/(1-t)$ and $u(T_2) = 0$. Using the same conventions, $T_1 + T_2$ has coordinates $[0 : 1 : -j]$ in Hesse form and abscissa $u(T_1 + T_2) = -j/(1 - jt)$ in projection from the origin.

In particular the quantity:

$$\frac{x(T_1 + T_2) - x(T_2)}{x(T_1 + T_2) - x(T_1)} = \frac{1-t}{j+2}$$

is invariant by affine transformations.

Compute the affine transformation mapping $1/(1-t)$ and 1 to $u(T_1)$ and $u(T_2)$, and returns the transformed equation $y^2 = P'(x)$.

Normalize y to obtain the Weierstrass form of Hessian curve $y^2 = p_3x^3 + p_2x^2 + p_1x + p_0$ where $p_1 + p_2 = 1$. This is done by ensuring that $y(T_1) = -1/(1-t)$.

function CurveParams(E: $y^2 = P(x)$, $T_1 \in E[3]$, $T_2 \in E[3]$, $j \in \mu_3$)
  Assert WeilPairing(T_1, T_2) = j
  $x_1, x_2, x_{12} \leftarrow x(T_1), x(T_2), x(T_1 + T_2)$
  $t \leftarrow -(j+2)(x_{12} - x_2)/(x_{12} - x_1)$
  $a \leftarrow (x_2 - x_1)(1/t - 1)$
  $b \leftarrow x_2 - a$
  $c \leftarrow (t-1)y(T_1)$
  $P' \leftarrow P(ax + b)/c^2$
  Assert $3t^3P' = 4(1-t^3)x^3 + 3(t^3-4)x^2 + 12x - 4$
  return t, $(x, y) \mapsto (ax + b, cy)$, P'
end function

Step 2. Compute singularities coordinates. The singularities of the image of H in $\mathbb{P}^1 \times \mathbb{P}^1$ are entirely known by explicit formulas given above. They are 8 rational functions of total degree 3 in t_1 and t_2.

If there is a triple point, 2 of these double points will be equal.

function DoubleCoords($j \in \mu_3$, t_1, t_2)
  $u_0 \leftarrow (t_1t_2 - 1)/(t_1^3 - 1)$
  $n_1 \leftarrow t_1^2 - j^2t_1t_2 - t_2 + j^2$
  $u_1 \leftarrow n_1/(n_1 + jt_1(1 - t_1t_2))$
  $n_2 \leftarrow t_1^2 - jt_1t_2 - t_2 + j$
  $u_2 \leftarrow n_2/(n_2 + j^2t_1(1 - t_1t_2))$
  $n_3 \leftarrow t_1^2 - t_1t_2 - t_2 + 1$

$u_3 \leftarrow n_3/(n_3 + t_1(1 - t_1t_2))$
return u_0, u_1, u_2, u_3
end function
function DoublePoints($j \in \mu_3$, t_1, t_2)
$u_0, u_1, u_2, u_3 \leftarrow$ DoubleCoords(j, t_1, t_2)
$v_0, v_1, v_2, v_3 \leftarrow$ DoubleCoords(j^2, t_2, t_1)
if any $(u_i, v_i) = (u_j, v_j)$ for $i \neq j$ **then**
return triple point, double point
else
return (u_i, v_i) for $i = 0, 1, 2, 3$
end if
end function

Step 3. Compute a sextic equation for H_ι. The normalised Weierstrass polynomials and the coordinates of the 4 double points provide $3 \times 4 + 6 = 18$ constraints on the 16 coefficients of polynomials of degree $(3, 3)$.

If there is a triple point, the 3 second order derivatives give a total of $6+3\times2+3 = 15$ constraints only.

This is an overdetermined linear system: a matrix kernel computation provides the equation in the general case. In the case of a triple point, the matrix is square.

function RationalSextic(P_1, P_2, Nodes $= N_0, \ldots, N_3$ or N_0 (triple), N_1)
$a_3x^3 + a_2x^2 + a_1x + a_0 \leftarrow P_1(x)$
$b_3x^3 + b_2x^2 + b_1x + b_0 \leftarrow P_2(x)$
$B(u, v) \leftarrow a_3b_3u^3v^3 + b_3v^3(a_2u^2 + a_1u + a_0) + a_3u^3(b_2v^2 + b_1v + b_0)$
$M \leftarrow$ Matrix(9, 12)
$V \leftarrow$ Vector(12)
for $k \leftarrow 0 \ldots \text{len(Nodes)} - 1$ **do**
for $(i, j) \leftarrow (0, 0) \ldots (2, 2)$ **do**
$m(u, v) \leftarrow u^iv^j$
$M[3i + j][3k] \leftarrow m(N_k)$
$M[3i + j][3k + 1] \leftarrow \partial m/\partial u(N_k)$
$M[3i + j][3k + 2] \leftarrow \partial m/\partial v(N_k)$
end for
$V[3k] \leftarrow -B(N_k)$
$V[3k + 1] \leftarrow -\partial B/\partial u(N_k)$
$V[3k + 2] \leftarrow -\partial B/\partial v(N_k)$
end for
if N_0 is a triple point **then**
$M[6][3k] \leftarrow \partial m/\partial u^2(N_0)$
$M[7][3k + 1] \leftarrow \partial m/\partial v^2(N_0)$
$M[8][3k + 2] \leftarrow \partial m/\partial u\partial v(N_0)$
$V[6] \leftarrow -\partial B/\partial u^2(N_k)$
$V[7] \leftarrow -\partial B/\partial v^2(N_0)$
$V[8] \leftarrow -\partial B/\partial u\partial v(N_0)$
end if
$Q \leftarrow$ Solve(MQ = V)
return $B + \sum Q[3i + j]u^iv^j$
end function

Step 4. Compute a rational parameterisation. The first quadratic transformation uses the base triangle formed by the x and y axes through one of the singular points (and the line at infinity), if the source is assumed to be compactified as $\mathbb{P}^2$. If the

source is viewed as $\mathbb{P}^1 \times \mathbb{P}^1$ the operation consists in blowing up the singular point and contracting the x and y lines through that point.

The second quadratic transformation has base triangle the remaining 3 singular points.

The image of the curves through these transformations is a conic which is easily rationally parameterised. This gives the two degree 3 rational functions N_1/D_1 and N_2/D_2 defining the projections from H_ι to $E_{i,\iota}$.

Note that the standard quadratic transformation $(x, y, z) \mapsto (xy, yz, zx)$ does not involve any operation on coefficients and can be computed only on each monomial.

The algorithm requires an oracle providing coordinates of a rational point on the final conic. It can be done by random sampling on a finite field (which needs square roots) or by using a known rational point (the Weierstrass points at infinity can be used if they are known).

If there is a triple point, after the first quadratic transformation the curve will already be a rational nodal cubic instead of a 3-nodal quartic, and it can be readily parameterised using the double point node as the origin.

The successive transformations are:

- S: the original sextic;
- S_1: a translation of S so that N_0 is the affine plane origin;
- Q: the image by a standard quadratic transformation;
- Q_T: a projective transformation of Q moving N_1, N_2, N_3 to $[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]$;
- C: a smoooth conic obtained from Q_T by the standard quadratic transformation;
- C_T: a translated conic so that a chosen rational point is the origin.

function RationalParams(Sextic, Nodes $= N_0, N_1, N_2, N_3$ or N_0 (triple), N_1)
  $S(x, y, z) \leftarrow$ Homogenize(Sextic)
  $x_0, y_0 \leftarrow N_0$
  $S_1(x, y, z) \leftarrow S(x_0 z + x, y_0 z + y, z)$ ▷ Translate N_0 to point $(0, 0)$
  $Q(x, y, z) \leftarrow S_1(yz, zx, xy)$ ▷ Apply quadratic transform
  $Q \leftarrow Q/x^3y^3z^2$ ▷ Remove exceptional lines
  if N_0 is a triple point **then**
    $Q \leftarrow Q/z$ ▷ Q is a cubic with node N_1
    $ax^2 + bxy + cy^2 + kx^3 + lx^2y + mxy^2 + ny^3 \leftarrow C(x_{P_C} + x, y_{P_C} + y, 1)$
    $x_Q(T) \leftarrow -(a + bT + cT^2)/(k + lT + mT^2 + nT^3)$
    $y_Q(T) \leftarrow Tx_Q(T)$
    $(x_Q(T), y_Q(T)) \leftarrow (x_{P_Q} + x_Q(T), y_{P_Q} + y_Q(T))$
    $x_Q(T), y_Q(T), z_Q(T) \leftarrow$ Homogenize$(x_Q(T), y_Q(T))$
  else
    $M \leftarrow$ Matrix$((x, y, z) \mapsto xN_1 + yN_2 + zN_3)$
    $Q_T(x, y, z) \leftarrow Q(M(x, y, z))$ ▷ Move N_i to basis vectors
    $C(x, y, z) \leftarrow Q_T(yz, zx, xy)/x^2y^2z^2$ ▷ C is a conic
    $P_C \leftarrow$ FindPoint(C) ▷ Find a rational point on C
    $ax^2 + bxy + cy^2 + dx + ey \leftarrow C(x_{P_C} + x, y_{P_C} + y, 1) = 0$
    $x_C(T) \leftarrow -(d + eT)/(a + bT + cT^2)$
    $y_C(T) \leftarrow Tx_C(T)$
    $(x_C(T), y_C(T)) \leftarrow (x_{P_C} + x_C(T), y_{P_C} + y_C(T))$ ▷ Then clear denominator
    $x_C(T), y_C(T), z_C(T) \leftarrow$ Homogenize$(x_C(T), y_C(T))$
    $(x_{Q_T}, y_{Q_T}, z_{Q_T}) \leftarrow (y_C z_C, z_C x_C, x_C y_C)$
    $(x_Q, y_Q, z_Q) \leftarrow M^{-1}(x_{Q_T}, y_{Q_T}, z_{Q_T})$
  end if
  $(x_{S_1}, y_{S_1}, z_{S_1}) \leftarrow (y_Q z_Q, z_Q x_Q, x_Q y_Q)$

return $(x_0 + x_{S_1}/z_{S_1}, y_0 + y_{S_1}/z_{S_1})$
end function

Step 5. Compute final morphisms. Using the rational functions above, and following computations done in the previous section, we can define the main function of the algorithm.

function TripleCover((E_1, T_{11}, T_{12}), (E_2, T_{21}, T_{22}))
$j \leftarrow$ WeilPairing(T_{11}, T_{12})
$t_1, f_1, P_1 \leftarrow$ CurveParams(E_1, T_{11}, T_{12}, j)
$t_2, f_2, P_2 \leftarrow$ CurveParams(E_2, T_{21}, T_{22}, j)
Nodes $\leftarrow$ DoublePoints(j, t_1, t_2)
$S \leftarrow$ RationalSextic$(P_1, P_2,$ Nodes$)$
$\mathrm{NX}_1 / \mathrm{DX}_1, \mathrm{NX}_2 / \mathrm{DX}_2 \leftarrow$ RationalParams(S, Nodes)
$a_1 \leftarrow P_1(\mathrm{NX}_1(\infty)/\mathrm{DX}_1(\infty))$
$a_2 \leftarrow P_2(\mathrm{NX}_2(\infty)/\mathrm{DX}_2(\infty))$
$R_1 \leftarrow \sqrt{P_1(\mathrm{NX}_1/\mathrm{DX}_1)\,\mathrm{DX}_1^3/(a_1\,\mathrm{DX}_2)}$ ▷ Square root of a monic polynomial
$R_2 \leftarrow \sqrt{P_2(\mathrm{NX}_2/\mathrm{DX}_2)\,\mathrm{DX}_2^3/(a_2\,\mathrm{DX}_1)}$ ▷ Square root of a monic polynomial
$a \leftarrow \sqrt{a_1 a_2}$ ▷ Square root of a field element
$H \leftarrow a_1\,\mathrm{DX}_1\,\mathrm{DX}_2$
$p_1 \leftarrow$ **map** $(x, y) \mapsto (f_1(\mathrm{NX}_1(x)/\mathrm{DX}_1(x)), yR_1(x)/\mathrm{DX}_1(x)^2)$
$p_2 \leftarrow$ **map** $(x, y) \mapsto (f_2(\mathrm{NX}_2(x)/\mathrm{DX}_2(x)), (a_2/a)yR_2(x)/\mathrm{DX}_2(x)^2)$
return H, p_1, p_2
end function

Appendix: Sagemath implementation

The implementation was tested on the whole parameter space for $\mathbb{F}_q$ where $q \bmod 6 = 1$ and $q \leq 200$. It returns either the equation of a hyperelliptic curve and 2 morphisms to the input elliptic curves, or an error if the triple cover is found to be singular.

Step 1: compute Hesse pencil parameter

```
def curve_params(E, j, T1, T2):
    xT1 = T1[0]
    xT2 = T2[0]
    xT12 = (T1 + T2)[0]
    t = (-j-2) * (xT12-xT2) / (xT12-xT1) + 1
    a = (xT1 - xT2) * (t - 1)
    b = xT2

    a1, a2, a3, a4, a6 = E.a_invariants()
    assert a1 == 0 and a3 == 0
    x = E.base_field()["x"].gen()
    P = (a*x+b)**3 + a2*(a*x+b)**2 + a4*(a*x+b) + a6
    return t, P, a, b
```

Step 2: compute singularities coordinates

```
def double_coords(j, t1, t2):
    d0 = (t1**2 - t2) / (t1**3 - 1)
    num1 = j*(t1*t2 - 1)
    den1 = num1*t1 - (t1**2 - j**2*t1*t2 - t2 + j**2)
    num2 = j**2*(t1*t2 - 1)
    den2 = num2*t1 - (t1**2 - j*t1*t2 - t2 + j)
    num3 = t1*t2 - 1
    den3 = num3*t1 - (t1**2 - t1*t2 - t2 + 1)
```

```
    return d0, num1 / den1, num2 / den2, num3 / den3

def double_points(j, t1, t2):
    XD0, XD1, XD2, XD3 = double_coords(j, t1, t2)
    YD0, YD1, YD2, YD3 = double_coords(j**2, t2, t1)
    nodes = [(XD0, YD0), (XD1, YD1), (XD2, YD2), (XD3, YD3)]
    if nodes[0] == nodes[1]:
        return [nodes[0]] + [n for n in nodes if n != nodes[0]]
    if nodes[2] == nodes[3]:
        return [nodes[2]] + [n for n in nodes if n != nodes[2]]
    return nodes
```

Step 3: equation of the plane rational sextic

```
def rational_sextic(P1, P2, nodes):
    assert P1[3] == 1 and P2[3] == 1
    K = P1.base_ring()
    R = K["u", "v"]
    u, v = R.gens()
    # Information from lines at infinity
    S_inf = u**3*v**3 \
        + (v**3 * (u**2*P1[2] + u*P1[1] + P1[0])) \
        + (u**3 * (v**2*P2[2] + v*P2[1] + P2[0]))
    dS_du = derivative(S_inf, u)
    dS_dv = derivative(S_inf, v)

    rows = []
    vals = []
    degrees = [(i, j) for i in range(3) for j in range(3)]
    for xN, yN in nodes:
        rows.append([xN**i * yN**j for i, j in degrees])
        vals.append(-K(S_inf(u=xN, v=yN)))
        rows.append([i*xN**(i-1)*yN**j if i > 0 else 0 for i, j in degrees])
        vals.append(-K(dS_du(u=xN, v=yN)))
        rows.append([j*xN**i*yN**(j-1) if j > 0 else 0 for i, j in degrees])
        vals.append(-K(dS_dv(u=xN, v=yN)))
    if len(nodes) == 2: # triple point
        dS_du2 = derivative(dS_du, u)
        dS_duv = derivative(dS_du, v)
        dS_dv2 = derivative(dS_dv, v)
        xN, yN = nodes[0]
        vals.append(-K(dS_du2(u=xN, v=yN)))
        rows.append([2 * yN**j if i == 2 else 0 for i, j in degrees])
        vals.append(-K(dS_dv2(u=xN, v=yN)))
        rows.append([2 * xN**i if j == 2 else 0 for i, j in degrees])
        vals.append(-K(dS_duv(u=xN, v=yN)))
        rows.append([0, 0, 0, 0, 1, 2*yN, 0, 2*xN, 4*xN*yN])

    M = Matrix(K, rows)
    coef = M.solve_right(vector(K, vals))
    S_rest = sum(c * u**i * v**j for c, (i, j) in zip(coef, degrees))
    return S_inf + S_rest
```

Step 4: compute a rational parameterisation of the sextic

```
def rational_params(S, nodes):
    K = S.base_ring()
    R = K["x", "y", "z"]
    x, y, z = R.gens()
```

```
    x0, y0 = nodes[0]
    S = S(x, y).homogenize(var=z)
    S1 = S(x + x0*z, y + y0*z, z)

    Q = div_monom(S1(y*z, z*x, x*y), x**3 * y**3 * z**2)
    T = K["T"].gen() # Uniformizer
    if len(nodes) == 2: # triple point
        Q = div_monom(Q, z) # nodal cubic
        x1, y1 = nodes[1]
        qx1, qy1, qz1 = (y1-y0, x1-x0, (x1-x0)*(y1-y0))
        QT = Q(qx1 * z + x, qy1 * z + y, qz1 * z)
        num = QT[2,0,1] + QT[1,1,1]*T + QT[0,2,1]*T**2
        den = QT[3,0,0] + QT[2,1,0]*T + QT[1,2,0]*T**2 + QT[0,3,0]*T**3
        xQT, yQT, zQT = -num, -num*T, den
        x_Q, y_Q, z_Q = qx1 * zQT + xQT, qy1 * zQT + yQT, qz1 * zQT
    else:
        (x1, y1), (x2, y2), (x3, y3) = nodes[1:4]
        M = Matrix(K, [
            [y1-y0, x1-x0, (x1-x0)*(y1-y0)],
            [y2-y0, x2-x0, (x2-x0)*(y2-y0)],
            [y3-y0, x3-x0, (x3-x0)*(y3-y0)],
        ]).transpose()
        u, v, w = M * vector([x, y, z])
        QT = Q(u, v, w)
        C = div_monom(QT(y*z, z*x, y*x), (x*y*z) ** 2)
        assert C.total_degree() == 2
        # Choose a rational point, assuming a finite field
        rat = Conic(C).rational_point()

        CT = C(rat[0]*z + x, rat[1]*z + y, z)
        # CT: ax^2+bxy+cy^2+dx+ey=0
        num = CT[1,0,1] + CT[0,1,1]*T
        den = CT[2,0,0] + CT[1,1,0]*T + CT[0,2,0]*T**2
        x_CT, y_CT, z_CT = -num, -T*num, den
        x_C, y_C, z_C = x_CT+rat[0]*z_CT, y_CT+rat[1]*z_CT, z_CT
        x_QT, y_QT, z_QT = y_C*z_C, z_C*x_C, x_C*y_C
        x_Q, y_Q, z_Q = M*vector([x_QT, y_QT, z_QT])
    x_S1, y_S1, z_S1 = y_Q*z_Q, z_Q*x_Q, x_Q*y_Q
    X = x0 + x_S1 / z_S1
    Y = y0 + y_S1 / z_S1
    return X, Y

def div_monom(f, q):
    R = f.parent()
    res = 0
    for c, m in zip(f.coefficients(), f.monomials()):
        assert R.monomial_divides(q, m)
        res += c * R.monomial_quotient(m, q)
    return res
```

Step 5: compute final equations

```
def triple_cover(E1, T11, T12, E2, T21, T22):
    K = E1.base_field()
    j = T11.weil_pairing(T12, 3)
    assert j == T21.weil_pairing(T22, 3)
    t1, P1, a1, b1 = curve_params(E1, j, T11, T12)
```

```
    t2, P2, a2, b2 = curve_params(E2, j, T21, T22)
    nodes = double_points(j, t1, t2)
    S = rational_sextic(P1.monic(), P2.monic(), nodes)
    X1, X2 = rational_params(S, nodes)
    NumX1, DenX1 = X1.numerator(), X1.denominator()
    NumX2, DenX2 = X2.numerator(), X2.denominator()
    if max(pol.degree() for pol in [NumX1, DenX1, NumX2, DenX2]) <= 2:
        return "H␣is␣singular", None, None
    Z1 = (P1(NumX1 / DenX1) * DenX1**3).numerator() // DenX2
    aZ1 = Z1.lc()
    Y1 = Z1.monic().sqrt()
    Z2 = (P2(NumX2 / DenX2) * DenX2**3).numerator() // DenX1
    aZ2 = Z2.lc()
    Y2 = Z2.monic().sqrt()
    aZ12 = (aZ1*aZ2).sqrt()

    def f1(x, y):
        return (a1*NumX1(x)/DenX1(x)+b1, Y1(x)/DenX1(x)**2 * y)
    def f2(x, y):
        return (a2*NumX2(x)/DenX2(x)+b2, Y2(x)/DenX2(x)**2 * y * aZ2 / aZ12)
    H = aZ1*DenX1*DenX2
    return H, f1, f2
```

Sample program and output

```
from sage.all import GF, EllipticCurve

K = GF(4099)
R = K["x", "y"]
x, y = R.gens()
E1 = EllipticCurve(K, [-961, -1125])
T11, T12 = E1.abelian_group().torsion_subgroup(3).gens()
E2 = EllipticCurve(K, [1044, 354])
T21, T22 = E2.abelian_group().torsion_subgroup(3).gens()

H, f1, f2 = triple_cover(
  E1, T11.element(), T12.element(),
  E2, T21.element(), T22.element())
print("H:", H)
# shows 2641*T^6+3151*T^5+2443*T^4+1911*T^3+3286*T^2+3446*T+3655
print("H->E1:", f1(x, y))
# shows
# (880*x^3 + 671*x^2 - 1915*x - 231)/(x^3 - 765*x^2 + 1818*x + 731)
# y*(x^3 - 1219*x^2 - 1118*x + 1170)/(x^3 - 765*x^2 + 1818*x + 731)^2
print("H->E2:", f2(x, y))
# shows
# (1625*x^3 - 496*x^2 - 172*x - 983)/(x^3 - 432*x^2 + 380*x + 149)
# y*(1937*x^3-1580*x^2-245*x-1525)/(405*(x^3 - 432*x^2 + 380*x + 149)^2)
```

References

[AD09] Michela Artebani and Igor V. Dolgachev, *The Hesse pencil of plane cubic curves*, Enseign. Math. **55** (2009), no. 3, 235–273, DOI 10.4171/LEM/55-3-3, available at https://ems.press/journals/lem/articles/12146.

[BFT14] Nils Bruin, Victor E. Flynn, and Damiano Testa, *Descent via (3,3)-isogeny on Jacobians of genus 2 curves*, Acta Arithmetica **165** (2014), no. 3, 201–223, DOI 10.4064/aa165-3-1, available at https://arxiv.org/abs/1401.0580.

[BHLS15] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, *Genus-2 curves and Jacobians with a given number of points*, LMS Journal of Computation and Mathematics **18** (2015), no. 1, 170–197, DOI 10.1112/s1461157014000461, available at `https://arxiv.org/abs/1403.6911`.

[BM] Araceli Bonifant and John Milnor, *On Real and Complex Cubic Curves*, available at `https://arxiv.org/abs/1603.09018`.

[CD21] Wouter Castryck and Thomas Decru, *Multiradical isogenies*, Cryptology ePrint Archive **2021/1133** (2021), available at `https://eprint.iacr.org/2021/1133`.

[CD22] Wouter Castryck and Thomas Decru, *An efficient key recovery attack on SIDH (preliminary version)*, Cryptology ePrint Archive **2022/975** (2022), available at `https://eprint.iacr.org/2022/975`.

[Dol12] Igor V. Dolgachev, *Classical Algebraic Geometry: a modern view*, Cambridge University Press, 2012.

[CR15] Romain Cosset and Damien Robert, *Computing (l, l)-isogenies in polynomial time on Jacobians of genus 2 curves*, Math. Comp. **84** (2015), 1953–1975, DOI 10.1090/S0025-5718-2014-02899-8, available at `https://hal.archives-ouvertes.fr/hal-00578991/file/niveau.pdf`.

[LR] David Lubicz and Damien Robert, *Arithmetic on Abelian and Kummer Varieties*, available at `https://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf`.

[Gau07] Pierrick Gaudry, *Fast genus 2 arithmetic based on Theta functions*, Journal of Mathematical Cryptology **1** (2007), no. 3, 243–265, DOI doi:10.1515/JMC.2007.012, available at `https://doi.org/10.1515/JMC.2007.012`.

[Kan97] Ernst Kani, *The number of curves of genus 2 with elliptic differentials*, J. reine angew. Math **485** (1997), 93–121, available at `https://mast.queensu.ca/~kani/papers/numgenl.pdf`.

[Kuh88] Robert M. Kuhn, *Curves of Genus 2 with Split Jacobian*, Transactions of the American Mathematical Society **307** (1988), no. 1, 41–49, available at `https://doi.org/10.1090/S0002-9947-1988-0936803-3`.

[Kun22] Sabrina Kunzweiler, *Efficient Computation of $(2^n, 2^n)$-Isogenies*, Cryptology ePrint Archive, Paper 2022/990 (2022), available at `https://eprint.iacr.org/2022/990`.

[Kuw11] Masato Kuwata, *Constructing families of elliptic curves with prescribed mod 3 representation via Hessian and Cayleyan curves* (2011), available at `https://arxiv.org/abs/1112.6317`.

[Mir85] Rick Miranda, *Triple Covers in Algebraic Geometry*, American Journal of Mathematics **107** (1985), no. 5, 1123–1158, DOI 10.2307/2374349.

[MW12] Dustin Moody and Hongfeng Wu, *Families of elliptic curves with rational 3-torsion*, Journal of Mathematical Cryptology **5** (2012), no. 3-4, 225–246, DOI doi:10.1515/jmc-2011-0013, available at `https://doi.org/10.1515/jmc-2011-0013`.

[SAGE] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 9.6)*, 2022. `https://www.sagemath.org`.

[Sha04] Tony Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280, available at `https://arxiv.org/abs/math/0109155`.

[DGPS22] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR *4-3-0 — A computer algebra system for polynomial computations*, 2022. `http://www.singular.uni-kl.de`.

[Smi05] Benjamin Smith, *Explicit Endormorphisms and Correspondences (PhD dissertation)* (2005), available at `http://iml.univ-mrs.fr/~kohel/phd/thesis_smith.pdf`.

[Roh05] Jan Christian Rohde, *Short equations for the genus 2 covers of degree 3 of an elliptic curve* (2005), available at `https://arxiv.org/abs/math/0503412`.

Email address: `remyoudompheng@gmail.com`