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 [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 $X_0(3)$), with canonical sections for the 3-torsion points at coordinates $[1 : -\zeta^k : 0], [0 : 1 : -\zeta^k], [-\zeta^k : 0 : 1]$, where $\zeta$ 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 $E_\lambda$ 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 $k$ and possesses 9 rational flex points, this projective equivalence can be realised over $k$.

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 $\zeta$ 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 \( k \)).

### 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 \( E_1 \to \text{Sym}^3 E_2 \to \text{Jac} E_2 \simeq E_2 \) 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 \( \text{Proj} E \) 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:

\[
\begin{array}{ccc}
H' & \to & L' \\
\downarrow & & \downarrow \\
E_1 \times E_2 & \overset{\pi_1}{\longrightarrow} & \mathbb{P}^2 \\
\downarrow & & \downarrow \\
\mathbb{P}^1 & \underset{u_1}{\longleftarrow} & \mathbb{P}^1 \\
\end{array}
\]

where \( L \) is a bundle of lines (a \( \mathbb{P}^1 \)-fibration over \( E_1 \)) which is the pullback of the incidence variety \( Q = \{ (\ell, P) \text{ such that } P \in \ell \} \subset (\mathbb{P}^2)^\vee \times \mathbb{P}^2 \), 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 \( L \) which is a degree 3 cover of \( E_1 \).

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

\[
\begin{array}{ccc}
E_1 & \overset{x_1}{\longrightarrow} & \mathbb{P}^1 \\
\downarrow & & \downarrow \\
\mathbb{P}^1 & \underset{u_1}{\longleftarrow} & \mathbb{P}^1 \\
\end{array}
\begin{array}{ccc}
H \subset E_1 \times E_2 & \overset{x_2}{\longrightarrow} & E_2 \subset \mathbb{P}^2 \\
\downarrow & & \downarrow \\
\mathbb{P}^1 & \underset{u_2}{\longleftarrow} & \mathbb{P}^1 \\
\end{array}
\]

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

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 \( \{ C_1, \ldots, C_6 \} \) 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

\[ Q = \{(P, \ell) \text{ such that } P \in \ell \} \subset \mathbb{P}^2 \times \left(\mathbb{P}^2\right)^\vee \]

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 \( \ell_P \) 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:

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

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:

\[
\begin{align*}
\gamma_1 &: ([x_1 : y_1 : z_1], [x_2 : y_2 : z_2]) \mapsto ([z_1 : x_1 : y_1], [z_2 : x_2 : y_2]) \\
\gamma_2 &: ([x_1 : y_1 : z_1], [x_2 : y_2 : z_2]) \mapsto ([x_1 : jy_1 : j^2 z_1], [x_2 : j^2 y_2 : jz_2])
\end{align*}
\]

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 \( \Gamma \), 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 \( \ell_{p_2} \) and \( \ell_{p_1} \).

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 \( x_1 x_2 + y_1 y_2 + z_1 z_2 \) 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 \( \ell_1 \).

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 \( E_1 \) at this point has coordinates: \( [x^2 - t y z : y^2 - t z x : z^2 - t y x] = [1 : 1 : t] \) which belongs to the pencil member \( E_1 \mu \) for \( \mu = (t^3 + 2)/(3t) \).

Moreover, since \( [1 : 1 : t] \) lies on line \( \{x = y\} \) it is a Weierstrass point on \( E_1 \).

The curve \( E_1 \mu \) is known as the Cayleyan curve of \( E_1 \) 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 \( E_1 \) be a Hessian cubic curve, and let \( \tau \) 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 \( E_\mu \) 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 \( P \in E_1 \), \( P \) and \( \tau(P) \) are conjugates to \( f(P) \in E_\mu \).

If \( \tilde{H} \) is the triple cover of \( E_1 \) and \( E_\mu \) defined by the polarity relation, the latter property implies the existence of a section \( E_1 \to \tilde{H} \) 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 \( \phi \) and the (translated) graph of the dual isogeny.

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

According to the secant group law, since \( \phi(P) = \phi(P + \epsilon) = Q \), the polar line \( \ell_Q \) 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 \( \phi \)) and \((-2P - \epsilon, Q) = (-\phi^*(Q) - \epsilon, Q)\) (belonging to the translated graph of the dual isogeny \( \phi^* \)).

In particular, \( \tilde{H} \) is the union of 2 irreducible components isomorphic to \( E_{\lambda} \) and \( E_{\mu} \).

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

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 \( \Gamma \) 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 \( \Gamma \) 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:

\[
X = x^6 y^3 + y^6 z^3 + z^6 x^3 - 3x^3 y^3 z^3
\]

\[
Y = x^3 y^6 + y^3 z^6 + z^3 x^6 - 3x^3 y^3 z^3
\]

\[
Z = xyz(x^6 + y^6 + z^6 - x^3 y^3 - y^3 z^3 - z^3 x^3)
\]

3.1. The genus 2 triple cover as a quotient correspondence. We have established that the polarity conjugacy relation defines a \( \Gamma \)-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:

\[
\begin{array}{ccc}
E_1 & \xrightarrow{[3]} & \tilde{H} & \xrightarrow{/\Gamma} & E_2 \\
\downarrow & & \downarrow /\Gamma & & \downarrow & \downarrow \ \\
E_1 & \xrightarrow{[3]} & H & \xrightarrow{/\Gamma} & E_2
\end{array}
\]

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 $E_1 \times E_2 \to \text{Jac } H$ 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 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 $\ell^1_P$ will be used (and $\ell^2_Q$ 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 bilinear relation $b_{t_1, t_2}$. For the polar line w.r.t. the origin 0, we can define the projection from the origin with formula $z/(x + y + zt)$, which is invariant by the bilinear relation $b_{t_1, t_2}$.

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 $(2g - 2 = C \cdot (C + K_{\mathbb{P}^1 \times \mathbb{P}^1}) = (3, 3) \cdot (1, 1) = 6)$. 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 $(L^2 = (L + E)^2 - 2L \cdot E - E^2 = \ldots$
Choosing the point at infinity \((\infty, \infty)\) 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 \(H_i\) 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 \(H\) 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 \(\phi\) has degrees \((1,2)\) with respect to the projections, and the graph of \(\phi^*\) has degree \((2,1)\). These graphs are invariant by action of \(\Gamma\) 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 \(E_2^T\) is a secant of \(E_2\), the line \(E_1^T\) is tangent to \(E_2\) at 3Q. By \(\Gamma\) invariance, we observe that if \(\tilde{H}\) contains \((P, Q)\) and \((P, Q + T)\), it also contains \((P - T, Q)\) thus the polar line \(E_1^T\) 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 \(\Gamma\)-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 \(\Gamma\), 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 \(LP\) 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 same \(\Gamma\)-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:

\[ \begin{array}{ccc}
P^2 & \xrightarrow{Q} & P^2 \\
\downarrow & & \downarrow \\
S(3) & \xrightarrow{Q_H} & S(3) \\
\downarrow & & \downarrow \\
P^1 & \xrightarrow{P^1 \times P^1} & P^1
\end{array} \]

where \( Q \) is the quadric defined by the polarity relation and the downward arrow are quotients under the action of \( \Gamma \), and \( S(3) \) is the blow-up of \( P^2 \) 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 \( P^1 \times P^1 \) corresponding to pairs of smooth elliptic curves \((t \neq \infty \text{ and } t^3 \neq 1)\), 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 \( k \) is fixed for these computation, in order to distinguish cases where the geometric situation (over \( \bar{k} \)) 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 \([x : y : z] \in E_2\)):

\[
\begin{align*}
u & = xyz \\
v & = x^6y^3 + y^6z^3 + z^6x^3 \\
w & = x^3y^6 + y^3z^6 + z^3x^6 \\
X & = v - 3u^3 \\
Y & = w - 3u^3 \\
tZ & = 9(t^3 - 1)w^3 - v - w
\end{align*}
\]

Polynomials with \( \Gamma \)-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) \( t_p \) is tangent to \( E_2 \) (see section 2.3). The set of ramification points is invariant under the hyperelliptic involution and the action of \( \Gamma \), 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 \((\mathbb{P}^2)^\vee \cong \mathbb{P}^2\).
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]:

\[ E_1 : x^3 + y^3 + z^3 = 3t_1xyz \]
\[ E_2 : x^3 + y^3 + z^3 = 3t_2xyz \]
\[ E_2' : x^6 + y^6 + z^6 + (4t_2^3 - 2)(x^3y^3 + y^3z^3 + z^3x^3) - 6t_2^2xyz(x^3 + y^3 + z^3) + (12t_2 - 3t_2^4)x^2y^2z^2 = 0 \]

Using intermediate coordinates

\[ u = xyz \]
\[ v = x^6y^3 + y^6z^3 + z^6x^3 \]
\[ z = x^3y^6 + y^3z^6 + z^3x^6 \]

we can find a low-degree member of the ideal of \( E_1 \cap E_2' \) using a computer-assisted computation:

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

to obtain a linear equation in the quotient plane:

\[ \tau = t_2^4 + 6t_1t_2^2 + t_1^2 - 4t_2 \]
\[ (X + Y)(4t_2^2t_3^2 - \tau) = Z(\tau t_1 - 4t_1^3 + 4 - 4t_2^2) \]

for the ramification of \( H \rightarrow E_2 \).

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 \( H \rightarrow E_1 \).

In general, this relation is not symmetric (the image of \( H \) in \( P^1 \times P^1 \) 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 \( P^1 \times P^1 \) are the images of the intersection of \( E_1 \) with the twisted duals of \( E_2 \) defined in section 3.3.

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

By symmetry, \( E_2' = E_2'' \).

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

\[ E_2' : (xy)^3 + (yz)^3 + (zx)^3 - 3t(x^2y^2z^2) = 0 \]
\[ E_2' : x^6 + y^6 + z^6 + (3jt - 1)(x^3y^3 + y^3z^3 + z^3x^3) - 3j(jt + 1)(x^4yz + y^4zx + z^4yx) + (3jxyz)^2 = 0 \]
\[ E_2' : x^6 + y^6 + z^6 + (3j^2t - 1)(x^3y^3 + y^3z^3 + z^3x^3) - 3j^2(j^2t + 1)(x^4yz + y^4zx + z^4yx) + (3j^2xyz)^2 = 0 \]
\[ E_2' : x^6 + y^6 + z^6 + (3t - 1)(x^3y^3 + y^3z^3 + z^3x^3) - 3(t + 1)(x^4yz + y^4zx + z^4yx) + (3xyz)^2 = 0 \]

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:

\[ L_0 : (x + y)(t_1^2 - t_2) - z(t_1 t_2 - 1) = 0 \]
\[ L_1 : (x + y)(jt_1 t_2 - j) + z(t_1^2 - j^2 t_1 t_2 - t_2 + j^2) = 0 \]
\[ L_2 : (x + y)(j^2 t_1 t_2 - j^2) + z(t_1^2 - j t_1 t_2 - t_2 + j) = 0 \]
\[ L_3 : (x + y)(t_1 t_2 - 1) + z(t_1^2 - t_1 t_2 - t_2 + 1) = 0 \]

The equation of \( E_2^{00} \) 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 \( \Delta \) in the Hesse configuration.

The equations above are defined over the base field \( k \) and define \( k \)-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 \( k \).

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 parameters;
3. for each \((t_1, t_2)\) determine orthogonal pairs \( P \in E_1 \) and its polar line \( \ell_P \)
   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 \( \leq 4 \) 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 \( \mathbb{F}_{2^{25}} \)) 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 \( \bar{H} \) (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:

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

\[
m_{00} = 3t_1^3 t_2^3 - 3t_1^2 t_2^2 - 2t_1^3 - 2t_2^3 + 3t_1 t_2 + 1
\]
\[
m_{01} = t_1^3 + t_2^3 - 3t_1^2 t_2 + 3t_1 t_2 - 2
\]
\[
m_{02} = t_1^3 - 3t_1^2 t_2 + 3t_1 t_2^2 + t_1 t_2 - 2t_1
\]
\[
m_{20} = t_2^3 - 3t_1^2 t_2 + 3t_1 t_2^2 + t_1 t_2 - 2t_2
\]
\[
m_{22} = t_1^3 t_2 + t_1 t_2^3 + 3t_1^2 t_2^2 - 3t_1^3 - 3t_2^3 - 2t_1 t_2 + 3
\]
\[
det M = (t_1^3 - 1)^3(t_2^3 - 1)^2(t_1 t_2 - 1)
\]
\[
\times (t_1 + t_2 + 1)(t_1 + j^2 t_2 + j)(t_1 + j t_2 + j^2) \quad \text{where} \quad j^3 = 1
\]

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 $H_i$ 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 $u/u' = z_1/(x_1 + y_1 + t_1z_1)$ and $u/v' = z_2/(x_2 + y_2 + t_2z_2)$ are affine coordinates for $E_1/i$ and $E_2/i$.

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

In addition to that, the first coordinate of double points has been computed earlier, so a linear relation $(x + y)A + zB = 0$ gives $u = A/(t_1A - B)$:

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

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

**Theorem 4.2.** Assuming the equation of $H$, it is normalised as

\[
u^3v^3 + v^3(a_{2,1}u^2v^2 + a_{4,1}uv^2 + a_{6,1}u^3) + u^3(a_{2,2}u^2v^2 + a_{4,2}uv^2 + a_{6,2}u^3) + u^3F(u, u', v, v')
\]

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 $(H_i)$ 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 $H/ι \to E_i/ι$ 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 $k$ is finite, $H$ has at least one non-Weierstrass rational point $(e_1, e_2) \times E_1 \times E_2$.

Proof. Since 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 $q + 1 - \text{Tr}(E_1) - \text{Tr}(E_2) > q - 4\sqrt{q}$ (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:

$$T \mapsto \left(\frac{NX_1(T)}{DX_1(T)}, \frac{NX_2(T)}{DX_2(T)}\right) \in H_i \subset \mathbb{P}^1 \times \mathbb{P}^1$$

realising a birational map from $\mathbb{P}^1$ to $H_i$. 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, $NX_2/DX_2$ maps the roots of $DX_1$ to the coordinates of the Weierstrass points of $E_2$, and conversely. These 6 points of $H_i$ are known to be the Weierstrass points of $H$ [Kub88].

Following equations given in [Kub88, BHLS15], we are looking for an equation $y_H^2 = \alpha DX_1(x_H)DX_2(x_H)$ for some scalar constant $\alpha$ 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:

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

Lemma 4.4. The polynomial $P_1(NX_1/DX_1)DX_1^3$ 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 $\mathbb{P}^1 \to H_i$ 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 $P_1(NX_1/DX_1)$ correspond to the $T$-coordinates of Weierstrass points of $E_1$, so $P_1(NX_1/DX_1)DX_1^2$ is a degree 9 effective divisor on $\mathbb{P}^1$ containing $\text{div} DX_2$. 
The complement consists of 3 pairs of points which are the other preimages of the Weierstrass points of $E_1$ in $H$, and since they are exchanged by the action of $\iota$, they map to a point of multiplicity 2 ($H_\iota$ is tangent to the line $\{x = x(W_{1,i})\}$), implying that this divisor has a square root. \hfill $\Box$

Note that since
\[(x^3 + ax^2 + bx + c)^2 = x^6 + 2ax^5 + (2b + a^2)x^4 + (2c + 2ab)x^3 + \ldots\]
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 $P_1(NX_1 / DX_1) DX_3^2$ which is $\alpha_1 = P_1(NX_1(\infty) / DX_1(\infty))$.

Since $P_1(NX_1 / DX_1) DX_3^2 = \alpha_1 DX_2 R_1^2$, this allows to define a map:
\[
(x_H, y_H) \mapsto \left( \frac{NX_1(x_H)}{DX_1(x_H)}, y_H \frac{R_1(x_H)}{DX_1(x_H)^2} \right)
\]
satisfying the relation:
\[
\left( y_H \frac{R_1(x_H)}{DX_1(x_H)^2} \right)^2 = \alpha DX_1(x_H) DX_2(x_H) \frac{R_1(x_H)^2}{DX_1(x_H)^2} = (\alpha/\alpha_1) P_1(NX_1(x_H)/DX_1(x_H))
\]

Let $(\epsilon_1, \epsilon_2) \in E_1 \times E_2$ be the image of a $k$-rational point of $H$ which is not a Weierstrass point of $H$ ($y(\epsilon_1) \neq 0$ and $y(\epsilon_2) \neq 0$). If $k$ is a finite field, this point is guaranteed to exist. Then $(x(\epsilon_1), x(\epsilon_2)) \in \mathbb{P}^1 \times \mathbb{P}^1$ is represented by a value of parameter $T \in \mathbb{P}^1(k)$ and the following identities hold:
\[
\begin{align*}
\alpha_1 DX_1(T) DX_2(T) \frac{R_1(T)^2}{DX_1(T)^4} &= P_1(NX_1(T) / DX_1(T)) = y(\epsilon_1)^2 \\
\alpha_2 DX_2(T) DX_1(T) \frac{R_2(T)^2}{DX_2(T)^4} &= P_2(NX_2(T) / DX_2(T)) = y(\epsilon_2)^2
\end{align*}
\]
meaning that $\alpha_1 \alpha_2$ is a square:
\[
\alpha_1 \alpha_2 = \left( \frac{y(\epsilon_1)y(\epsilon_2) DX_1(T) DX_2(T)}{R_1(T) R_2(T)} \right)^2
\]
As a consequence, we can define the following final equations:
\[
H : y^2 = \alpha_1 DX_1(x) DX_2(x)
\]

\[
H \mapsto E_1 : (x, y) \mapsto \left( \frac{NX_1(x)}{DX_1(x)}, y \frac{R_1(x)}{DX_1(x)^2} \right)
\]

\[
H \mapsto E_2 : (x, y) \mapsto \left( \frac{NX_2(x)}{DX_2(x)}, \frac{\alpha_2}{\sqrt{\alpha_1 \alpha_2}} y \frac{R_2(x)}{DX_2(x)^2} \right)
\]

4.7. An algorithm to compute the triple cover from elliptic curves with level structure. In the above calculations, we 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 $H_i \subset \mathbb{P}^1 \times \mathbb{P}^1$ using explicit formulas.
3. Compute the sextic model of $H_i$ 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 $H$, 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 $y^2 = p_1x^3 + p_2x^2 + p_1x + p_0$ 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 $\leftarrow -(j + 2)((x_1 - x_2)/(x_{12} - x_1))$

$a \leftarrow (x_2 - x_1)(1/t - 1)$

$b \leftarrow x_2 - a$

c $\leftarrow (t - 1)g(T_1)$

$P' \leftarrow P(ax + b)/c^2$

**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($j \in \mu_3$, $t_1, t_2$)

$u_0 \leftarrow (t_1t_2 - 1)/(t_1^2 - 1)$

$n_1 \leftarrow t_1^2 - j^2t_1t_2 - t_2 + j^2$

$n_1 \leftarrow n_1/(n_1 + j(t_1(1 - t_1t_2)))$

$n_2 \leftarrow t_1^2 - jt_1t_2 - t_2 + 2$

$n_2 \leftarrow n_2/(n_2 + j^2t_1(1 - t_1t_2))$

$n_3 \leftarrow t_1^2 - t_1t_2 - t_2 + 1$
\[ u_3 \leftarrow n_3/(n_3 + t_1(1 - t_1 t_2)) \]

\[
\text{return } u_0, u_1, u_2, u_3
\]

end function

function DoublePoints(j ∈ µ3, t1, t2)
\[ u_0, u_1, u_2, u_3 \leftarrow \text{DoubleCoords}(j, t_1, t_2) \]
\[ v_0, v_1, v_2, v_3 \leftarrow \text{DoubleCoords}(j^2, t_2, t_1) \]
if any \((u_i, v_i) = (u_j, v_j)\) for \(i \neq j\)

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 \(H_1\). The normalised Weierstrass polynomials and the coordinates of the 4 double points provide 3 × 4 + 6 = 18 constraints on the 16 coefficients of polynomials of degree (3, 3).

If there is a triple point, the 5 second order derivatives give a total of 6+3×2+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(P1, P2, Nodes \(= N_0, \ldots, N_3\) or \(N_0\) (triple), \(N_1\))
\[
a_3 x^3 + a_2 x^2 + a_1 x + a_0 \leftarrow P_1(x)
\]
\[
b_3 x^3 + b_2 x^2 + b_1 x + b_0 \leftarrow P_2(x)
\]
\[
B(u, v) \leftarrow a_3 b_3 u^3 v^3 + b_3 v^3 (a_2 u^2 + a_1 u + a_0) + a_3 w^3 (b_2 v^2 + b_1 v + b_0)
\]
\[
M \leftarrow \text{Matrix}(9, 12)
\]
\[
V \leftarrow \text{Vector}(12)
\]
for \(k \leftarrow 0\ldots\text{len}(\text{Nodes}) - 1\)

for \((i, j) \leftarrow (0, 0) \ldots (2, 2)\)

\[
m(u, v) \leftarrow u^i v^j
\]
\[
M[3i + j][3k] \leftarrow m(N_k)
\]
\[
M[3i + j][3k + 1] \leftarrow \partial m/\partial u(N_k)
\]
\[
M[3i + j][3k + 2] \leftarrow \partial m/\partial v(N_k)
\]
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

\[
M[6][3k] \leftarrow \partial m/\partial u^2(N_0)
\]
\[
M[7][3k + 1] \leftarrow \partial m/\partial v^2(N_0)
\]
\[
M[8][3k + 2] \leftarrow \partial m/\partial u \partial v(N_0)
\]
\[
V[6] \leftarrow -\partial B/\partial u^2(N_0)
\]
\[
V[7] \leftarrow -\partial B/\partial v^2(N_0)
\]
\[
V[8] \leftarrow -\partial B/\partial u \partial v(N_0)
\]
end if

\[
Q \leftarrow \text{Solve}(MQ = V)
\]

return \(B + \sum Q[3i + j]u^i v^j\)
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 $H_1$ to $E_{\epsilon_1}$.

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 smooth conic obtained from $Q_T$ by the standard quadratic transformation;
- $C_T$: a translated conic so that a chosen rational point is the origin.

```plaintext
function RationalParams(Sextic, Nodes = N0, N1, N2, N3 or N0 (triple), N1)
    S(x, y, z) ← Homogenize(Sextic)
    x0, y0 ← N0
    S1(x, y, z) ← S(x0z + x, y0z + y, z)  ▷ Translate N0 to point (0, 0)
    Q(x, y, z) ← S1(yz, zx, xy)  ▷ Apply quadratic transform
    Q ← Q/x^3y^2z^2  ▷ Remove exceptional lines
    if N0 is a triple point then
        Q ← Q/z  ▷ Q is a cubic with node $N_1$
        ax^2 + bxy + cy^2 + kx^3 + lx^2y + mxy^2 + ny^3 ← C(xpc + x, ypc + y, 1)
        xQ(T) ← (a + bT + cT^2)/(k + IT + mT^2 + nT^3)
        yQ(T) ← TxQ(T)
        (xQ(T), yQ(T)) ← (xQ + xQ(T), yQ + yQ(T))
        xQ(T), yQ(T), zQ(T) ← Homogenize(xQ(T), yQ(T))
    else
        M ← Matrix((x, y, z) ← xN1 + yN2 + zN3)
        QT(x, y, z) ← Q(M(x, y, z))  ▷ Move N1 to basis vectors
        C(x, y, z) ← QT(yz, zx, xy)/x^2y^2z^2  ▷ C is a conic
        PC ← FindPoint(C)  ▷ Find a rational point on C
        ax^2 + bxy + cy^2 + dx + ey ← C(xpc + x, ypc + y, 1) = 0
        xc(T) ← (d + eT)/(a + bT + cT^2)
        yc(T) ← TxC(T)
        (xc(T), yc(T)) ← (xpc + xc(T), ypc + yc(T))  ▷ Then clear denominator
        C(xc(T), yc(T), zc(T) ← Homogenize(xc(T), yc(T))
        (xQr, yQr, zQr) ← (yc zc, zc xc, xc yc)
        (xQ, yQ, zQ) ← M^{-1}(xQr, yQr, zQr)
    end if
    (xs1, ys1, zs1) ← (yQzQ, zQxQ, xQyQ)
```

PROJECTIVE GEOMETRY OF HESSE CURVES AND TRIPLE COVERS 17
return \((x_0 + xS_1/zS_1, y_0 + yS_1/zS_1)\)

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 \text{T}riple\text{C}over((E_1, T_{11}, T_{12}), (E_2, T_{21}, T_{22}))

\(j \leftarrow \text{WeilPairing}(T_{11}, T_{12})\)
\(t_1, f_1, P_1 \leftarrow \text{CurveParams}(E_1, T_{11}, T_{12}, j)\)
\(t_2, f_2, P_2 \leftarrow \text{CurveParams}(E_2, T_{21}, T_{22}, j)\)

Nodes \(\leftarrow \text{DoublePoints}(j, t_1, t_2)\)
\(S \leftarrow \text{RationalSextic}(P_1, P_2, \text{Nodes})\)
\(NX_1 / DX_1, NX_2 / DX_2 \leftarrow \text{RationalParams}(S, \text{Nodes})\)
\(a_1 \leftarrow P_1(NX_1(\infty)/DX_1(\infty))\)
\(a_2 \leftarrow P_2(NX_2(\infty)/DX_2(\infty))\)

\[R_1 \leftarrow q^{\sqrt{P_1(NX_1/DX_1) DX_3^2/(a_1 DX_2)}} \quad \triangleright \text{Square root of a monic polynomial}\]
\[R_2 \leftarrow q^{\sqrt{P_2(NX_2/DX_2) DX_3^2/(a_2 DX_1)}} \quad \triangleright \text{Square root of a monic polynomial}\]
\[a \leftarrow \sqrt{a_1 a_2} \quad \triangleright \text{Square root of a field element}\]
\(H \leftarrow a_1 DX_1 DX_2\)
\(p_1 \leftarrow \text{map}(x, y) \mapsto (f_1(NX_1(x)/DX_1(x)), gR_1(x)/DX_1(x)^2)\)
\(p_2 \leftarrow \text{map}(x, y) \mapsto (f_2(NX_2(x)/DX_2(x)), (a_2/a)gR_2(x)/DX_2(x)^2)\)

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 \(q \mod 6 = 1\) 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

```python
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

```python
def double_coords(j, t1, t2):
d0 = (t1**2 - t2) / (t1**3 - 1)
um1 = 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 - ti*t2 - t2 + 1)
```
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):
    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, 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()
\[ x_0, y_0 = \text{nodes}[0] \]
\[ S = S(x, y).\text{homogenize}(\text{var}=z) \]
\[ S_1 = S(x + x_0*z, y + y_0*z, z) \]
\[ Q = \text{div\_monom}(S_1(y*z, z*x, x*y), x**3 * y**3 * z**2) \]
\[ T = K["T"].\text{gen()} \] # Uniformizer

if len(nodes) == 2: # triple point
    Q = \text{div\_monom}(Q, z) # nodal cubic
    x_1, y_1 = nodes[1]
    qx_1, qy_1, qz_1 = (y_1-y_0, x_1-x_0, (x_1-x_0)*(y_1-y_0))
    QT = Q(qx_1 * z + x, qy_1 * z + y, qz_1 * 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
    x_QT, y_QT, z_QT = -num, -num*T, den
    x_Q, y_Q, z_Q = qx_1 * z_QT + x_QT, qy_1 * z_QT + y_QT, qz_1 * z_QT
else:
    (x_1, y_1), (x_2, y_2), (x_3, y_3) = nodes[1:4]
    M = \text{Matrix}(K, [
        [y_1-y_0, x_1-x_0, (x_1-x_0)*(y_1-y_0)],
        [y_2-y_0, x_2-x_0, (x_2-x_0)*(y_2-y_0)],
        [y_3-y_0, x_3-x_0, (x_3-x_0)*(y_3-y_0)]
    ]).\text{transpose()}
    u, v, w = M * \text{vector}([x, y, z])
    QT = Q(u, v, w)
    C = \text{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 = \text{Conic}(C).\text{rational\_point()} 
    CT = C(rat[0]*z + x, rat[1]*z + y, z) # CT: ax^2+2bxy+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, -num*T, 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_S1, y_S1, z_S1 = y_Q*z_Q, z_Q*x_Q, x_Q*y_Q
    X = x_0 + x_S1 / z_S1
    Y = y_0 + 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.\text{weil\_pairing}(T12, 3)
    assert j == T21.\text{weil\_pairing}(T22, 3)
    t1, P1, a1, b1 = \text{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*x^6+3151*x^5+2443*x^4+1911*x^3+3286*x^2+3446*x+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*(z^3 - 1219*z^2 - 1118*z + 1170)/(z^3 - 765*z^2 + 1818*z + 731)^2
print("H->E2:", f2(x, y))
# shows
# (1625*z^3 - 496*z^2 - 172*z - 983)/(z^3 - 432*z^2 + 380*z + 149)
# y*(1937*z^3-1580*z^2-245*z-1525)/(405*(z^3 - 432*z^2 + 380*z + 149)^2)

References


Email address: remyoudompheng@gmail.com