Noname manuscript No.
(will be inserted by the editor)

Analogue of Vélu's Formulas for Computing Isogenies over Hessian Model of Elliptic Curves

Perez Broon Fouazou Lontouo · **Emmanuel Fouotsa**
·

Received: date / Accepted: date

Abstract Vélu's formulas for computing isogenies over Weierstrass model of elliptic curves has been extended to other models of elliptic curves such as the Huff model, the Edwards model and the Jacobi model of elliptic curves. This work continues this line of research by providing efficient formulas for computing isogenies over elliptic curves of Hessian form. We provide explicit formulas for computing isogenies of degree 3 and isogenies of degree ℓ not divisible by 3. The theoretical cost of computing these maps in this case is slightly faster than the case with other curves. We also extend the formulas to obtain isogenies over twisted and generalized Hessian forms of elliptic curves. The formulas in this work have been verified with the Sage software and are faster than previous results on the same curve.

Keywords Elliptic curves · Isogeny · Hessian curves · Vélu's formulas

Mathematics Subject Classification (2000) 14H52 · 14K02

1 Introduction

Isogenies are morphisms of finite nucleus groups between two elliptic curves. Given an elliptic curve E over a field $\mathbf{K}$ and a finite subgroup G of $E(\mathbf{K})$ the Vélu formulas [30] explicitly determine an elliptic curve E' and an isogeny from E to E' with kernel G. Isogenies are widely used in the study of elliptic curves [28]. They are also very used in elliptic curve cryptography in particular to accelerate the scalar multiplication over elliptic curves as shown in [13], [14], [8] and [23]. Isogenies are also used in the SEA algorithm to compute the cardinality of an elliptic curve [1], [12] and [26]. Also, mathematical primitives in the construction of cryptographic one-way functions such as hashes and pseudo-random

Perez Broon Fouazou Lontouo
Department of Mathematics and Computer Science
Faculty of Sciences
The University of Dschang P.O.Box 67 Dschang, Cameroon
E-mail: fouazouperez@gmail.com

Emmanuel Fouotsa
Department of Mathematics, Higher Teacher Training College,
The University of Bamenda, P.O BOX 39 Bambili, Cameroon
E-mail: emmanuelfouotsa@yahoo.fr

number generators using isogenies have been proposed in [5] and [16]. More interestingly is the construction of a quantum-resistant public crypto-systems based on super-singular elliptic curves isogenies (SIDH) [10]. The research works previously cited are based mostly on the classical Weierstrass model of an elliptic curve. Several other models exist in the literature such as the Hessian model, the Edward model, the Jacobi model, the Huff model. These curves are almost all birationally equivalent to the Weierstrass model but depending on the properties of each curve such as arithmetic of points, a careful choice of the model may be necessary. For example, an elliptic curve with complete addition formulas and/or unified addition formulas ensures protection against exceptional procedure attacks [17] and side-channel attacks respectively on protocols based on the curves used. Also, addition formulas that can be parallelized may be preferable in term of efficiency of the computations. The Hessian model of elliptic curves [29] has been proven to have unified addition formulas [18] which can be computed in a parallel way [29]. Also this model presents a nice geometric interpretation of the group law that allows to obtain competitive costs in pairing's computation with respect to well known models of curves such as the Weierstrass and the Edward model [15], [11]. Also, some standard curves from IEEE, SECG can be transformed to Hessian curves as pointed out by Smart [29]. Analogues of Vélu's formulas for Edward, Huff and Jacobi models of elliptic curves are given in [24] and [31]. Expressing isogenies on other models of elliptic curves (Edward, Huff, Jacobi, Hessian ... .etc) can improve the efficiency of the considered algorithms. The computation of Isogenies over Edward elliptic curve has been improved in several works such as [20], [19] and in [2] to improve the efficiency of SIDH. Orhon et *al.* [25] provide a faster inversion-free point addition formulas using 2-isogenies on Huff curve. Meyer et *al.* [22] improved the efficiency of the commutative SIDH using Edward isogenies. Improved Isogenies over Edward curves are also used to ensure resistance against timing attack and fault injection attack on the commutative SIDH [4]. Isogenies over Montgomery curves have been used to propose a variant of the CGL hash [5] that is faster than the original algorithm and preimage and collision resistant. The above discussion on the possible efficiency and alternate use of isogenies over different models of elliptic curves justify this work aiming to provide competitive formulas for isogenies over Hessian elliptic curves.

To our knowledge, only formulas for degree-2 isogenies exist over this curve [6]. At the time we are submitting this work, we are aware of the latest preprint [7] just uploaded online and computing also isogenies over Hessian curves. But the formulas for isogenies of odd degree $\ell = 2r+1$ are extremely costly $((5r+3)M+4S+8rC)$, which is even slower than Edward, Huff and Jacobi isogenies, contrary to the efficient formulas obtained in this work costing $((3r+3)M+3S+3rC)$ where M,S and C denote the cost of a field multiplication, squaring and multiplication by a constant. Also this work provides a fastest $(3M+3S+6C)$ degree-3 isogeny with respect to Edward $(6M+4S+3C)$, Huff $(7M+3S+4C)$ and Jacobi $(6M+3S+11C)$ isogenies. Furthermore we provide explicit formulas verified with the Sage script available in [21] for the Hessian curves, the generalized and the twisted Hessian curves both for degree 3 isogenies and odd degree ℓ isogenies.

The remainder of this document is be organized as follows: in Section 2 we will recall the Vélu formulas [30] as well as the definition and arithmetic of Hessian curve. In Section 3 we derive explicit formulas for isogenies of degree 3 over the Hessian Curves. The result is extended to the twisted and generalized Hessian curves. In Section 4 we treat the more general case of isogenies of degrees not divisible by 3. The Section 5 will be devoted to a comparison of the computational cost in term of basic fields operations of isogenies over Edward, Huff, Jacobi quartic and Hessian models of elliptic curves. The work is concluded in Section 6.

2 Background on Isogenies and Hessian Elliptic Curves

This section briefly recalls the Vélu formulas for computing isogenies over elliptic curves. The arithmetic over Hessian model and maps between twisted and generalized Hessian models of elliptic curves are described as well.
In what follows, **K** denotes a finite field with characteristic different from 2 and 3.

2.1 Review of Vélu's Formulas

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over **K** . Let ℓ be an odd prime and G an subgroup of order ℓ. The map ϕ defined by

$$\phi(P) = (x_P + \sum_{Q \in G - \{\infty\}} (x_{P+Q} - x_P), y_P + \sum_{Q \in G - \{\infty\}} (y_{P+Q} - y_P))$$

is invariant under translation by elements of G, and the kernel of ϕ is G. Using the group law on the curve, we also see that ϕ can be written in terms of rational functions. Indeed let $G^* = G - \{\infty\}$. Partitionning G into two sets G^+ and G^- such that $G^* = G^+ \cup G^-$, and $P \in G^+$ iff $-P \in G^-$ and for each point $P \in G^+$, we define the following quantities
$g^x_P = 3x_P^2 + a, g^y_P = -2y_P, v_P = 2g^x_P, u_P = (g^y_P)^2, v = \sum_{P \in G^+} v_P$ and $w = \sum_{P \in G^+} (u_P + x_P v_P)$, then the ℓ-isogeny $\phi : E \longrightarrow E'$ is given by

$$\phi(x,y) = \left(x + \sum_{P \in G^+} (\frac{v_P}{x - x_P} - \frac{u_P}{(x - x_P)^2}), y - \sum_{P \in G^+} (\frac{2yu_P}{(x - x_P)^3} + v_P \frac{y - y_P - g^x_P g^y_P}{(x - x_P)^2}) \right)$$

The equation for the image curve is $E' : y^2 = x^3 + (A - 5v)x + (B - 7w)$.

2.2 The Hessian Model of Elliptic Curve

2.2.1 The Hessian and the Generalized Hessian Elliptic Curve

Definition 1 [18] A Hessian curve over **K** is a cubic equation $H_d : X^3 + Y^3 + Z^3 = dXYZ$ in the projective space $P^2(\mathbf{K})$ with $d \in \mathbf{K}$ and $d^3 \neq 27$. The affine equation is given by $H_d : x^3 + y^3 + 1 = dxy$.

The generalized Hessian curve which cover more isomorphism classes of elliptic curves than Hessian curves is defined in [9].

Definition 2 [9] Let c, d be elements of **K** such that $c \neq 0$ and $d^3 \neq 27c$. The generalized Hessian curve $H_{c,d}$ over **K** is defined by the equation

$$H_{c,d} : X^3 + Y^3 + cZ^3 = dXYZ.$$

Clearly, a Hessian curve H_d is a generalized Hessian curve $H_{c,d}$ with $c = 1$. Moreover, a generalized Hessian curve $H_{c,d}$ over **K** is isomorphic over $\bar{K}$ to the Hessian curve $H_{d/\sqrt[3]{c}}$: $\tilde{x}^3 + \tilde{y}^3 + 1 = (d/\sqrt[3]{c})\tilde{x}\tilde{y}$ via the map $f : (x; y) \mapsto (\tilde{x}; \tilde{y})$ defined by $\tilde{x} = x/\sqrt[3]{c}$ and $\tilde{y} = y/\sqrt[3]{c}$ with $\sqrt[3]{c}^3 = c$. The inverse is $f^{-1}(x,y) = (\sqrt[3]{c}x, \sqrt[3]{c}y)$. The common j-invariant is $j(H_{c,d}) = j(H_{d/\sqrt[3]{c}}) = \frac{1}{c}\left(\frac{d(d^3+6^3c)}{d^3-3^3c}\right)^3$.

Remark 1 .

1. $H_{c,d}$ has exactly three points at infinity $(1:-1:0),(1:-j:0)$ and $(1:-j^2:0)$ with $j^2+j+1=0$. In characteristic 3 there is only one point at infinity $(1:-1:0)$.
2. By putting $x=y$ we show that the points whose ordinate is equal to the abscissa satisfy $2x^3+c-dx^2=2y^3+c-dy^2=0$.
3. By putting $x=0$ (resp $y=0$) on $H_{c,d}$, we obtain the points $(0:-\sqrt[3]{c}:1)$ (resp $(-\sqrt[3]{c}:0:1)$)with $\sqrt[3]{c}^3=c$. In the particular case of Hessian curve $H_{1,d}$, if $car(k)\neq 3$ we have the points $(0:-1:1),(0:-j:1)$ *and* $(0:-j^2:1)$ (resp $(-1:0:1),(-j:0:1)$ *and* $(-j^2:0:1)$)with $j^2+j+1=0$. In characteristic 3 there is only one point $(0:-1:1)$ (resp $(-1:0:1)$)

2.2.2 Addition Formulas on Hessian Elliptic Curves

Unified addition formulas on generalized Hessian elliptic curve are given in [9]. Given two points $(X_1:Y_1:Z_1)$ and $(X_2:Y_2:Z_2)$ on the curve, their sum is the point $(X_3:Y_3:Z_3)$ given by

$$(X_3:Y_3:Z_3)=(cY_2Z_2Z_1^2-X_1Y_1X_2^2:X_2Y_2Y_1^2-cX_1Z_1Z_2^2:X_2Z_2X_1^2-Y_1Z_1Y_2^2)$$

Remark 2 .

1. $(1:-1:0)$ is the neutral element and inverse of $(X:Y:Z)$ is $(Y:X:Z)$.
2. the points of order 2 are the points whose ordinate is equal to the abscissa.
3. $(X:Y:Z)+(-\sqrt[3]{c}:0:1)=(\sqrt[3]{c}Y:\sqrt[3]{c}^2Z:X)$ (we suppose $X\neq 0$), $(X:Y:Z)+(0:-\sqrt[3]{c}:1)=(\sqrt[3]{c}^2Z:\sqrt[3]{c}X:Y)$ (we suppose $Y\neq 0$) and $(X:Y:Z)+(1:-j:0)=(jX:j^2Y:Z)$
4. For each $\sqrt[3]{c}\in\bar{k}$ such that $\sqrt[3]{c}^3=c$, $\{(1:-1:0),(-\sqrt[3]{c}:0:1),(0:-\sqrt[3]{c}:1)\}$ is a sub-group of order 3.
5. If $car(k)\neq 3$, The three points at infinity form a sub-group of order 3 $\{(1:-1:0),(1:-j:0),(1:-j^2:0)\}$.

2.2.3 Birational Transformation and Twisted Hessian Curves

We note that the elliptic curve E over $\mathbf{K}$ has a point of order 3 if and only if it has a Weierstrass model $E_{a_1,a_3}: y^2z+a_1xyz+a_3yz^2=x^3$ [3] .

Theorem 1 *[9] Let E be an elliptic curve over* $\mathbf{K}$. *If the group* $E(\mathbf{K})$ *has a point of order 3 then E is isomorphic over* $\mathbf{K}(j)$ *(with* $j^2+j+1=0$*) to a generalized Hessian curve . More precisely* $E: y^2z+a_1xyz+a_3yz^2=x^3$ *is isomorphic over* $\mathbf{K}(j)$ *to the generalized Hessian curve* $H_{c,d}: x^3+y^3+c=dxy$ *where* $d=3a_1$ *and* $c=a_1^3-27a_3$ *via the map:*
$\varphi_{c,d}(X:Y:Z)=(ja_1X+(j-1)Y+(2j+1)a_3Z:-(j+1)a_1X-(j+2)Y-(2j+1)a_3Z:X)$
from E to $H_{c,d}$ *and inverse transformation is given by*

$$\varphi_{c,d}^{-1}(X:Y:Z)=(3a_3Z:(-a_3)X+(-a_3)Y-a_1a_3Z:(-j)X+(j+1)Y-a_1Z)$$

The sage script available in [21, isom.ipynb] can be used to verify that $\varphi_{c,d}\circ\varphi_{c,d}^{-1}=Id_{H_{c,d}}$ and $\varphi_{c,d}^{-1}\circ\varphi_{c,d}=Id_E$. We note that $\varphi_{c;d}$ is not a group isomorphism because $\varphi_{c,d}(0:1:0)=(1:-j^2:0)$. But using a translation one obtains $\varphi_d(X:Y:Z)+(1:-j:0)=(j^2a_1X+(-2j-1)Y+(-j-2)a_3Z:ja_1X+(2j+1)Y+(j-1)a_3Z:X)$ which is an isomorphism of group because $\varphi_{c,d}(0:1:0)+(1:-j:0)=(1:-1:0)$ and its inverse is $\varphi_{c,d}^{-1}((X:Y:Z)+(1:-j^2:0))=(3a_3Z:((j+1)a_3)X+(-ja_3)Y-a_1a_3Z:-X-Y-a_1Z)$

we can see that a uniformiser at neutral point $(1:-1:0)$ is $t=\frac{1}{((j+1))x+jy+a_1}=\frac{3}{3j^2x+3jy+d}$ for the future we will take $t=\frac{1}{3j^2x+3jy+d}$

Definition 3 [3] A projective twisted Hessian curve over $\mathbf{K}$ is a curve of the form $\mathscr{H}_{a,d}: aX^3+Y^3+Z^3=dXYZ$ in $\mathbf{P}^2(\mathbf{K})$ with specified point $(0:-1:1)$, where a and d are elements of $\mathbf{K}$ with $a(27a-d^3)\neq 0$.

We give here the addition formulas from [3] called rotated addition. The inverse of a point $(X_1:Y_1:Z_1)$ is $-(X_1:Y_1:Z_1)=(X_1:Z_1:Y_1)$ and the sum of two points $(X_1:Y_1:Z_1)$ and $(X_2:Y_2:Z_2)$ of $\mathscr{H}_{a,d}$ is the point $(X_3':Y_3':Z_3')$ defined by $X_3'=Z_2^2X_1Z_1-Y_1^2X_2Y_2, Y_3'=Y_2^2Y_1Z_1-aX_1^2X_2Z_2$ and $Z_3'=aX_2^2X_1Y_1-Z_1^2Y_2Z_2$. Points of twisted Hessian curve corresponding to $X=0$ (resp $Y=0$ or $Z=0$) are $(0:-1:1),(0:-j:1)$ and $(0:-j^2:1)$ (resp $(1:0:-\sqrt[3]{a})$ or $(1:-\sqrt[3]{a}:0)$) if $car(\mathbf{K})\neq 3$.$\{(0:-1:1),(0:-j:1),(0:-j^2:1)\}$ and $\{(0:-1:1),(1:0:-\sqrt[3]{a}),(1:-\sqrt[3]{a}:0)\}$ are the subgroups of order 3. The points of order 2 has coordinates $(\gamma,1)$ where $a\gamma^3+2-d\gamma=0$.

It is easy to establish the following Lemma 1 that gives an isomorphism between the twisted Hessian curve (provided of addition law of subsection 2.2.3) and generalized Hessian curve (provided of addition law of subsection 2.2.2).

Lemma 1 *The map f' defined by $f'(x,y)=(\frac{1}{x},\frac{y}{x})$ is an isomorphism from the twisted Hessian curve $\mathscr{H}_{a,d}$ to the generalized Hessian curve $H_{a,d}$. Its inverse is $f^{-1}(x,y)=(\frac{1}{x},\frac{y}{x})$*

3 Formulas for Isogenies of Degree 3 on Hessian Curve

In this section, we consider a Hessian curve H_d over $\mathbf{K}$ and we derive formulas for isogenies with kernel a subgroup of $H_d(\mathbf{K})$ of order 3. Furthermore we consider also a subgroup G of $H_d(\mathbf{K})$ of order an odd integer ℓ not divisible by 3 and we find an elliptic curve H_d' and an isogeny from H_d to H_d' with kernel G.

Theorem 2 *Let H_d be an Hessian curve over $\mathbf{K}$ and G a subgroup of $H_d(\mathbf{K})$ of order 3. We define a curve $H_{d'}$ and give an isogeny $g: H_d \longrightarrow H_{d'}$ of kernel G, for each possibility of G.*

(a) if $G=\{(1:-1:0),(-1,0),(0,-1)\}$ then the affine map

$$\begin{array}{rccc} g: & H_d & \longrightarrow & H_{d'} \\ & (x,y) & \mapsto & (m\frac{x+x^2y+y^2}{xy}, m\frac{y+y^2x+x^2}{xy}) \end{array}$$

projectively defined by

$$(X:Y:Z)\longmapsto (m(XZ^2+X^2Y+ZY^2):m(Z^2Y+Y^2X+ZX^2):XYZ)$$

is an isogeny of kernel G. The coefficient of the curve $H_{d'}$ is given by $d'=m(d+6)$ where $m^3=\frac{1}{d^2+3d+9}$

(b) *if* $G = \{(1:-1:0),(-j,0),(0,-j)\}$ *then* *the affine map*

$$\begin{array}{rccc} g: & H_d & \longrightarrow & H_{d'} \\ & (x,y) & \mapsto & (m\frac{jx+j^2x^2y+y^2}{xy}, m\frac{jy+j^2y^2x+x^2}{xy}) \end{array}$$

projectively defined by

$$(X:Y:Z) \longmapsto (m(jXZ^2+j^2X^2Y+ZY^2) : m(jZ^2Y+j^2Y^2X+ZX^2) : XYZ)$$

is an isogeny of kernel G. The coefficients of the curve $H_{d'}$ *is given by* $d' = m(j^2d+6)$ *where* $m^3 = \frac{1}{jd^2+3j^2d+9}$

(c) *if* $G = \{(1:-1:0),(-j^2,0),(0,-j^2)\}$ *then* *the affine map*

$$\begin{array}{rccc} g: & H_d & \longrightarrow & H_{d'} \\ & (x,y) & \mapsto & (m\frac{jx+x^2y+j^2y^2}{xy}, m\frac{jy+y^2x+j^2x^2}{xy}) \end{array}$$

projectively defined by

$$(X:Y:Z) \longmapsto (m(jXZ^2+X^2Y+j^2ZY^2) : m(jZ^2Y+Y^2X+j^2ZX^2) : XYZ)$$

is an isogeny of kernel G. The coefficients of the curve $H_{d'}$ *is given by* $d' = m(d+6j^2)$ *where* $m^3 = \frac{1}{j^2d^2+3jd+9}$

(d) *if* $G = \{(1:-1:0),(1:-j:0),(1:-j^2:0)\}$ *then the affine map*

$$\begin{array}{rccc} g: & H_d & \longrightarrow & H_{d'} \\ & (x,y) & \mapsto & (m\frac{-jx^3+1-d(-1/3j+1/3)xy}{xy}, m\frac{-jy^3+1-d(-1/3j+1/3)xy}{xy}) \end{array}$$

projectively defined by $(X:Y:Z) \longmapsto (m(-jX^3+Z^3-d(-1/3j+1/3)XYZ) : m(-jY^3+Z^3-d(-1/3j+1/3)XYZ) : XYZ)$ *is an isogeny of kernel G. The coefficients of the curve* $H_{d'}$ *is given by* $d' = dm(j+2)$ *where* $m^3 = -3\frac{2j+1}{d^3-27}$

Proof . The expressions of these maps are easily inspired from the composition of the isomorphism between Weierstrass and Hessian curves and the Weierstrass isogenies.

- Proof of the case (a) where $G = \{(1:-1:0),(-1,0),(0,-1)\}$ and $g(X:Y:Z) = (m(XZ^2+X^2Y+ZY^2) : m(Z^2Y+Y^2X+ZX^2) : XYZ)$. We start to show that for all $(x,y) \in H_d$, $g(x,y) \in H_{d'}$. After reducing the power of x greater than 3 in the numerator of $g_x^3+g_y^3+1-d'g_xg_y$ by using the equation of H_d and using the fact that $d' = m(d+6)$, $g_x^3+g_y^3+1-d'g_xg_y$ becomes $\frac{((-d^3-3d^2-9d)m^3+d)yx+((d^2+3d+9)m^3-1)y^3+(d^2+3d+9)m^3-1}{x^3}$ which is zero since $m^3 = \frac{1}{d^2+3d+9}$. The sage script available in [21, 3-isogenies.ipynb (first cell)] can be used to check the computation of numerator and denominator of $g_x^3+g_y^3+1-d'g_xg_y$. Also $g(1:-1:0) = g(-1:0:1) = g(0:-1:1) = (1:-1:0)$ so g is an isogeny and $G \subseteq ker(g)$. $g(1:-j:0) = (1:-j:0)$ and $g(1:-j^2:0) = (1:-j^2:0)$ so $(1:-j:0)$ and $(1:-j^2:0) \notin ker(g)$. $ker(g)$ does not contain a point at infinity. Let $(x,y) \in H_d$ so that $g(x,y) = (1:-1:0)$ using the projective form of g we have $xy = 0$ so, $(x,y) = \mp(-1,0), \mp(-j,0)$ or $\mp(-j^2,0)$ but $g((-j,0)) = g((-1,0)+(1:-j:0)) = (1:-j:0)$ and $g((-j^2,0)) = g((-1,0)+(1:-j^2:0)) = (1:-j^2:0)$ (since g is an isogeny) so $(x,y) = \mp(-1,0)$ and $G = ker(g)$.

- Proof of the case (b) where $G = \{(1:-1:0), (-j,0), (0,-j)\}$ and

$$g(X:Y:Z) = (m(jXZ^2 + j^2X^2Y + ZY^2) : m(jZ^2Y + j^2Y^2X + ZX^2) : XYZ)$$

  We start to show that for all $(x,y) \in H_d$, $g(x,y) \in H_{d'}$. After reducing the power of x greater than 3 in the numerator of $g_x^3 + g_y^3 + 1 - d'g_xg_y$ by using the equation of H_d and using the fact that $d' = m(j^2d+6)$, $g_x^3 + g_y^3 + 1 - d'g_xg_y$ becomes $\frac{((-jd^3+(3j+3)d^2-9d)m^3+d)yx+((jd^2+(-3j-3)d+9)m^3-1)y^3+(jd^2+(-3j-3)d+9)m^3-1}{x^3}$ which is zero since $m^3 = \frac{1}{jd^2+3j^2d+9}$. The sage script available in [21, 3-isogenies.ipynb (second cell)] can be used to check the computation of numerator and denominator of $g_x^3 + g_y^3 + 1 - d'g_xg_y$. Also $g(1:-1:0) = g(-j:0:1) = g(0:-j:1) = (1:-1:0)$ so g is an isogeny and $G \subseteq ker(g)$.
  $g(1:-j:0) = (1:-j:0)$ and $g(1:-j^2:0) = (1:-j^2:0)$ so $(1:-j:0)$ and $(1:-j^2:0)$ $\notin ker(g)$. $ker(g)$ does not contain a point at infinity.
  Let $(x,y) \in H_d$ so that $g(x,y) = (1:-1:0)$ using the projective form of g we have $xy = 0$ so, $(x,y) = \mp(-1,0), \mp(-j,0)$ or $\mp(-j^2,0)$ but $g((-1,0)) = g((-j,0)+(1:-j^2:0)) = (1:-j^2:0)$ and $g((-j^2,0)) = g((-j,0)+(1:-j:0)) = (1:-j:0)$ (since g is an isogeny) so $(x,y) = \mp(-j,0)$ and $G = ker(g)$.
- Proof of the case (c) where $G = \{(1:-1:0), (-j^2,0), (0,-j^2)\}$ and

$$g(X:Y:Z) = (m(jXZ^2 + X^2Y + j^2ZY^2) : m(jZ^2Y + Y^2X + j^2ZX^2) : XYZ)$$

  We start to show that for all $(x,y) \in H_d$, $g(x,y) \in H_{d'}$. After reducing the power of x greater than 3 in the numerator of $g_x^3 + g_y^3 + 1 - d'g_xg_y$ by using the equation of H_d and using the fact that$d' = m(d+6j^2)$, $g_x^3 + g_y^3 + 1 - d'g_xg_y$ becomes $\frac{(((-j^2)d^3-3jd^2-9d)m^3+d)yx+(((j^2)d^2+3jd+9)m^3-1)y^3+((j^2)d^2+3jd+9)m^3-1}{x^3}$ which is zero since $m^3 = \frac{1}{j^2d^2+3jd+9}$. The sage script available in [21, 3-isogenies.ipynb (third cell)] can be used to check the computation of numerator and denominator of $g_x^3 + g_y^3 + 1 - d'g_xg_y$. We also have that $g(1:-1:0) = g(-j^2:0:1) = g(0:-j^2:1) = (1:-1:0)$ so g is an isogeny and $G \subseteq ker(g)$. $g(1:-j:0) = (1:-j:0)$ and $g(1:-j^2:0) = (1:-j^2:0)$ so $(1:-j:0)$ and $(1:-j^2:0) \notin ker(g)$. $ker(g)$ does not contain a point at infinity. Let $(x,y) \in H_d$ so that $g(x,y) = (1:-1:0)$ using the projective form of g we have $xy = 0$ so, $(x,y) = \mp(-1,0), \mp(-j,0)$ or $\mp(-j^2,0)$ but $g((-1,0)) = g((-j^2,0)+(1:-j:0)) = (1:-j:0)$ and $g((-j,0)) = g((-j^2,0)+(1:-j^2:0)) = (1:-j^2:0)$ (since g is an isogeny) so $(x,y) = \mp(-j^2,0)$ and $G = ker(g)$.
- Proof of the case (d) where $G = \{(1:-1:0), (1:-j^2:0), (1:-j:0)\}$ and $g(X:Y:Z) = (m(-jX^3 + Z^3 - d(-1/3j+1/3)XYZ) : m(-jY^3 + Z^3 - d(-1/3j+1/3)XYZ) : XYZ)$
  We start to show that for all $(x,y) \in H_d$, $g(x,y) \in H_{d'}$. After reducing the power of x greater than 3 in the numerator of $g_x^3 + g_y^3 + 1 - d'g_xg_y$ by using the equation of H_d and using the fact that $d' = dm(j+2)$, $g_x^3 + g_y^3 + 1 - d'g_xg_y$ becomes $\frac{(((-\frac{2}{9}j-\frac{1}{9})d^4+(6j+3)d)m^3+d)yx+(((\frac{2}{9}j+\frac{1}{9})d^3+(-6j-3))m^3-1)y^3+((\frac{2}{9}j+\frac{1}{9})d^3+(-6j-3))m^3-1}{x^3}$ which is zero since $m^3 = -3\frac{2j+1}{d^3-27}$. The sage script available in
  [21, 3-isogenies.ipynb (fourth cell)] can be used to check the computation of numerator and denominator of $g_x^3 + g_y^3 + 1 - d'g_xg_y$. We also have that $g(1:-1:0) = g(1:-j^2:0) = g(1:-j:0) = (1:-1:0)$ so g is an isogeny and $G \subseteq ker(g)$. $g(-1:0:1) = (m(j+1):m:0) = (1:-j:0)$ and $g(0:-1:1) = (1:-j^2:0)$. Let $(x,y) \in H_d$ so that $g(x,y) = (1:-1:0)$ using the projective form of g we have $xy = 0$ so, $(x,y) =$

$\mp(-1,0), \mp(-j,0)$ or $\mp(-j^2,0)$ but $g((-j^2,0)) = g((-1,0)+(1:-j^2:0)) = (1:-j:0)$ and $g((-j,0)) = g((-1,0)+(1:-j:0)) = (1:-j:0)$ (since g is an isogeny) so $ker(g)$ does not have the point in affine coordinate $G = ker(g)$.

3.0.1 Generalization of Formulas to Generalized Hessian curve

Theorem 3 *Let $H_{c,d}$ be the generalized Hessian curve over the field* $\mathbf{K}$. *For each of the following subgroup G of $H_{c,d}(\mathbf{K})$ order 3 we give an isogeny $g' : H_{c,d} \longrightarrow H_{c',d'}$ of kernel G:*

(a) if $G = \{(-1:1:0), (0, -\sqrt[3]{c}), (-\sqrt[3]{c}:0)\}$ then

$$\begin{array}{rcl} g' : H_{c,d} & \longrightarrow & H_{c',d'} \\ (x,y) & \mapsto & \left(\frac{x^2y+\sqrt[3]{c}y^2+\sqrt[3]{c}^2x}{xy}, \frac{y^2x+\sqrt[3]{c}x^2+\sqrt[3]{c}^2y}{xy}\right) \end{array}$$

is an isogeny of kernel G. The coefficients of the curve $H_{c',d'}$ are given by $d' = d + 6\sqrt[3]{c}$ and $c' = d^2\sqrt[3]{c} + 3d\sqrt[3]{c}^2 + 9c$

(b) if $G = \{(0:-1:1), (0:-j:1), (0:-j^2:1)\}$ then

$$\begin{array}{rcl} g' : H_{c,d} & \longrightarrow & H_{c',d'} \\ (x,y) & \mapsto & \left(\frac{(-2j-1)x^3+(jd\sqrt[3]{c})xy+(-j+1)c}{xy}, \frac{(-2j-1)y^3+(jd\sqrt[3]{c})xy+(-j+1)c}{xy}\right) \end{array}$$

is an isogeny of kernel G. The coefficients of the curve $H_{c',d'}$ are given by $d' = 3d$ and $c' = d^3 - 27c$

Proof 1. Proof of part (a). Using the isomorphism $f : H_{c,d} \longrightarrow H_{d/\sqrt[3]{c}}$, $f(x,y) = (\frac{x}{\sqrt[3]{c}}, \frac{y}{\sqrt[3]{c}})$ (given in Subsection 2.2.1 between the generalized Hessian curve and the Hessian curve) the image of the subgroup $G = \{(1:-1:0), (0, -\sqrt[3]{c}), (-\sqrt[3]{c}, 0)\}$ is the subgroup $G' = \{(1:-1:0), (-1,0), (0,-1)\}$. We apply Theorem 2 (first case) to have an isogeny $g : H_{d/\sqrt[3]{c}} \longrightarrow H_{d_1}$, $g(x,y) = (m\frac{x+x^2y+y^2}{xy}, m\frac{y+y^2x+x^2}{xy})$ with $d_1 = m(\frac{d+6\sqrt[3]{c}}{\sqrt[3]{c}})$ and $m^3 = \frac{c}{d^2\sqrt[3]{c}+3d\sqrt[3]{c}^2+9c}$. So $d_1 = \frac{\sqrt[3]{c}}{\sqrt[3]{d^2\sqrt[3]{c}+3d\sqrt[3]{c}^2+9c}}(\frac{d+6\sqrt[3]{c}}{\sqrt[3]{c}}) = \frac{d+6\sqrt[3]{c}}{\sqrt[3]{d^2\sqrt[3]{c}+3d\sqrt[3]{c}^2+9c}}$. Using the inverse transformation $f^{-1} : H_{\frac{d+6\sqrt[3]{c}}{\sqrt[3]{d^2\sqrt[3]{c}+3d\sqrt[3]{c}^2+9c}}} \longrightarrow H_{d^2\sqrt[3]{c}+3d\sqrt[3]{c}^2+9c, d+6\sqrt[3]{c}}$ (given in Subsection 2.2.1 between generalized Hessian curve and Hessian curve) we have $f^{-1}(x,y) = (\sqrt[3]{d^2\sqrt[3]{c}+3d\sqrt[3]{c}^2+9c} \cdot x, \sqrt[3]{d^2\sqrt[3]{c}+3d\sqrt[3]{c}^2+9c} \cdot y)$ so that $f^{-1} \circ g \circ f(x,y) = (\frac{x^2y+\sqrt[3]{c}y^2+\sqrt[3]{c}^2x}{xy}, \frac{y^2x+\sqrt[3]{c}x^2+\sqrt[3]{c}^2y}{xy})$. The sage script available in [21, Extension_3isog.ipynb (first cell)] can be used for verification.

2. Proof of part (b). Using the isomorphism $f : H_{c,d} \longrightarrow H_{d/\sqrt[3]{c}}$, $f(x,y) = (\frac{x}{\sqrt[3]{c}}, \frac{y}{\sqrt[3]{c}})$ (given in Subsection 2.2.1 between the generalized Hessian curve and the Hessian curve) the image of the subgroup $G = \{(1:-1:0), (1:-j:0), (1:-j^2:0)\}$ (in the curve $H_{d/\sqrt[3]{c}}$) is the subgroup $G' = \{(1:-1:0), (1:-j:0), (1:-j^2:0)\}$. We apply Theorem 2 (fourth case) to have an isogeny $g : H_{d/\sqrt[3]{c}} \longrightarrow H_{d_1}$ defined by $g(x,y) = (m\frac{-jx^3+1-d(-1/3j+1/3)xy}{xy}, m\frac{-jy^3+1-d(-1/3j+1/3)xy}{xy})$ with $d_1 = m(j+2)\frac{d}{\sqrt[3]{c}}$ and $m^3 = -3c\frac{2j+1}{d^3-27c}$. So $m = \frac{\sqrt[3]{c}\sqrt[3]{-3(2j+1)}}{\sqrt[3]{d^3-27c}} = (-j+1)\frac{\sqrt[3]{c}}{\sqrt[3]{d^3-27c}}$ and $d_1 = (j+2)(-j+1)\frac{\sqrt[3]{c}}{\sqrt[3]{d^3-27c}}\frac{d}{\sqrt[3]{c}} = \frac{3d}{\sqrt[3]{d^3-27c}}$. By using the inverse transformation $f^{-1} : H_{\frac{3d}{\sqrt[3]{d^3-27c}}} \longrightarrow$

$H_{d^3-27c,3d}$ (given in Subsection 2.2.1 between the generalized Hessian curve and the Hessian curve) we have $f^{-1}(x,y) = (\sqrt[3]{d^3-27c}\cdot x, \sqrt[3]{d^3-27c}\cdot y)$ so that $f^{-1}\circ g\circ f(x,y) = (\frac{(-2j-1)x^3+(jd\sqrt[3]{c})xy+(-j+1)c}{xy}, \frac{(-2j-1)y^3+(jd\sqrt[3]{c})xy+(-j+1)c}{xy})$. The sage script available in [21, Extension_3isog.ipynb (second cell)] can be used to check calculation of $f^{-1}\circ g\circ f(x,y)$

3.0.2 Generalization of Formulas to Twisted Hessian curve

Theorem 4 *Let $\mathscr{H}_{a,d}$ be a twisted Hessian curve over $\mathbf{K}$. For the followings subgroups G of order 3 we give an isogeny $\mathbf{g}: \mathscr{H}_{a,d} \longrightarrow \mathscr{H}_{a',d'}$ of kernel G:*

(a) if $G = \{(0:-1:1),(1:0:-\sqrt[3]{a}),(1:-\sqrt[3]{a}:0)\}$ then

$$\begin{array}{rcl}\mathbf{g}: \mathscr{H}_{a,d} & \longrightarrow & \mathscr{H}_{a',d'}\\ (x,y) & \mapsto & (\frac{xy}{\sqrt[3]{a}xy^2+\sqrt[3]{a}^2x^2+y}, \frac{\sqrt[3]{a}^2x^2y+y^2+\sqrt[3]{a}x}{\sqrt[3]{a}xy^2+\sqrt[3]{a}^2x^2+y})\end{array}$$

is an isogeny of kernel G. The coefficients of the curve $\mathscr{H}_{a',d'}$ are given by $d' = d+6\sqrt[3]{a}$ and $a' = d^2\sqrt[3]{a}+3d\sqrt[3]{a}^2+9a$.

(b) $G = \{(0:-1:1),(0:-j:1),(0:-j^2:1)\}$ then

$$\begin{array}{rcl}\mathbf{g}: \mathscr{H}_{a,d} & \longrightarrow & \mathscr{H}_{a',d'}\\ (x,y) & \mapsto & (\frac{xy}{3ax^3+(j-1)d\sqrt[3]{a}xy-3j}, \frac{3ax^3-3jy^3+(j-1)d\sqrt[3]{a}xy}{3ax^3+(j-1)d\sqrt[3]{a}xy-3j})\end{array}$$

is an isogeny of kernel G. The coefficients of the curve $\mathscr{H}_{a',d'}$ are given by $a' = d^3-27a$ and $d' = 3d$.

Proof .

1. Proof of part (a). Using the isomorphism $f': \mathscr{H}_{a,d} \longrightarrow H_{a,d}$, $f'(x,y) = (\frac{1}{x}, \frac{y}{x})$ of Lemma 1, the image of the subgroup $G = \{(0:-1:1),(1:0:-\sqrt[3]{a}),(1:-\sqrt[3]{a}:0)\}$ is the subgroup $G' = \{(1:-1:0),(-\sqrt[3]{a},0),(0,-\sqrt[3]{a})\}$. We apply Theorem 3 (first case) to have an isogeny
$g': H_{a,d} \longrightarrow H_{d^2\sqrt[3]{a}+d\sqrt[3]{a}^2+9a,d+6\sqrt[3]{a}}$ defined by
$g(x,y) = (\frac{x^2y+\sqrt[3]{a}y^2+\sqrt[3]{a}^2x}{xy}, \frac{y^2x+\sqrt[3]{a}x^2+\sqrt[3]{a}^2y}{xy})$. The application of Lemma 1 gives the inverse transformation
$f'^{-1}: H_{d^2\sqrt[3]{a}+d\sqrt[3]{a}^2+9a,d+6\sqrt[3]{a}} \longrightarrow \mathscr{H}_{d^2\sqrt[3]{a}+d\sqrt[3]{a}^2+9a,d+6\sqrt[3]{a}}$ defined by
$f'^{-1}(x,y) = (\frac{1}{x}, \frac{y}{x})$ so that $f'^{-1}\circ g'\circ f'(x,y) = (\frac{xy}{\sqrt[3]{a}xy^2+\sqrt[3]{a}^2x^2+y}, \frac{\sqrt[3]{a}^2x^2y+y^2+\sqrt[3]{a}x}{\sqrt[3]{a}xy^2+\sqrt[3]{a}^2x^2+y})$ The sage script available in [21, Extension_3isog.ipynb (third cell)] can be used for the verification.
2. Proof of part (b).
Using the isomorphism $f': \mathscr{H}_{a,d} \longrightarrow H_{a,d}$, $f(x,y) = (\frac{1}{x}, \frac{y}{x})$ of Lemma 1 the image of the subgroup $G = \{(0:-1:1),(0:-j:1),(0:-j^2:1)\}$ is the subgroup $G' = \{(1:-1:0),(1:-j:0),(1:-j^2:0)\}$. We apply Theorem 3 (second case) to have an isogeny
$g': H_{a,d} \longrightarrow H_{d^3-27a,3d}$ defined by
$g'(x,y) = (\frac{(-2j-1)x^3+(jd\sqrt[3]{a})xy+(-j+1)a}{xy}, \frac{(-2j-1)y^3+(jd\sqrt[3]{a})xy+(-j+1)a}{xy})$. The application of Lemma 1 gives the inverse transformation

$f'^{-1}: H_{d^3-27a,3d} \longrightarrow \mathscr{H}_{d^3-27a,3d}$ defined by $f^{-1}(x,y) = (\frac{1}{x}, \frac{y}{x})$
so that $f'^{-1} \circ g' \circ f'(x,y) = (\frac{xy}{3ax^3+(j-1)d\sqrt[3]{a}xy-3j}, \frac{3ax^3-3jy^3+(j-1)d\sqrt[3]{a}xy}{3ax^3+(j-1)d\sqrt[3]{a}xy-3j})$. The sage script available in [21, Extension_3isog.ipynb (fourth cell)] can be used for the verification.

4 Formulas for Isogenies of Degree not Divisible by 3 over Hessian Elliptic Curves

In this section, we are given an Hessian elliptic curve H_d over $\mathbf{K}$ and G a subgroup of H_d of finite order ℓ non-divisible by 3. We then construct an elliptic curve H'_d defined over $\mathbf{K}$ and an explicit isogeny given in term of rational functions from H_d to $H_{d'}$ with kernel G. This formula is easily extended to twisted Hessian curves and generalized Hessian curve.
We throw out the neutral point $(1:-1:0)$ from G and denote $G^* = G - \{(1:-1:0)\}$. Let S be all the 2-torsion points of G^* and R be the rest of the points in G^*. We split R into two equal size sets R_- and R_+ so that a point P is in R_+ if and only if $-P$ is in R_-. We will take $r = \#R_-$ and $s = \#S$ so that $\ell = \#G = 2r+s+1$. we denote $S_{n,n-1}(x_1,x_2,...,x_n) = \sum_{1\le i_1<i_2...<i_{n-1}\le n} x_{i_1}x_{i_2}\cdots x_{i_{n-1}}$ the $(n-1)$-th elementary symmetric polynomial of $k[x_1,x_2,...,x_n]$.
For an arbitrary point $P \in H_d$ we define the map g by

$$g(P) = (\prod_{Q\in G} Y_{P+Q} : \prod_{Q\in G} X_{P+Q} : \prod_{Q\in G} Z_{P+Q}) \tag{1}$$

The following lemma is very important for the obtaining of an efficient ℓ-isogeny.

Lemma 2 *The map g is defined by*

$$g(x,y) = (y\prod_{(a,b)\in G^*}\frac{aby^2-x}{ax^2-b^2y}, x\prod_{(a,b)\in G^*}\frac{b-a^2xy}{ax^2-b^2y}) \tag{2}$$

and satisfies also the following

$$g(x,y) = (y\prod_{Q\in S}\frac{x_Q^2y^2-x}{x_Qx^2-x_Q^2y}\cdot\prod_{P\in R_-}\frac{x-x_Py_Py^2}{xy-x_Py_P}, x\prod_{Q\in S}\frac{1-x_Qxy}{x^2-x_Qy}\cdot\prod_{P\in R_-}\frac{y-x_Py_Px^2}{xy-x_Py_P}) \tag{3}$$

Proof We first observe that from equation (1) to equation (2) is a direct application of the group law. We now show the proof from equation (2) to equation (3).
Let $P(x_P,y_P) \in R_-$. Then $(x_Px^2-y_P^2y)(y_Px^2-x_P^2y) =$

$$\begin{aligned}
&= x_Py_Px^4 - x_P^3x^2y - y_P^3x^2y + x_P^2y_P^2y^2\\
&= x_Py_Px^4 - (x_P^3+y_P^3)x^2y + x_P^2y_P^2y^2\\
&= x_Py_Px(-y^3-1+dxy) - (-1+dx_Py_P)x^2y + x_P^2y_P^2y^2\\
&= -x_Py_Pxy^3 - x_Py_Px + dx_Py_Px^2y + x^2y - dx_Py_Px^2y + x_P^2y_P^2y^2\\
&= -x_Py_Pxy^3 - x_Py_Px + x^2y + x_P^2y_P^2y^2\\
&= x^2y - x_Py_Px - x_Py_Pxy^3 + x_P^2y_P^2y^2\\
&= (x - x_Py_Py^2)(xy - x_Py_P)
\end{aligned}$$

so that

$$(x_Px^2-y_P^2y)(y_Px^2-x_P^2y) = (x-x_Py_Py^2)(xy-x_Py_P) \tag{4}$$

$$\frac{x_Py_Py^2-x}{x_Px^2-y_P^2y}*\frac{x_Py_Py^2-x}{y_Px^2-x_P^2y} = \frac{(x_Py_Py^2-x)^2}{(x-x_Py_Py^2)(xy-x_Py_P)}$$
$$= \frac{x-x_Py_Py^2}{xy-x_Py_P}$$

We also have that

$$\begin{aligned}(y_P-x_P^2xy)(x_P-y_P^2xy) &= x_Py_P-y_P^3xy-x_P^3xy+x_P^2y_P^2x^2y^2\\ &= x_Py_P-(x_P^3+y_P^3)xy+x_P^2y_P^2x^2y^2\\ &= x_Py_P-(-1+dx_Py_P)xy+x_P^2y_P^2x^2y^2\\ &= x_Py_P+xy-dx_Py_Pxy+x_P^2y_P^2x^2y^2\end{aligned}$$

and

$$\begin{aligned}(y-x_Py_Px^2)(x-x_Py_Py^2) &= xy-x_Py_Px^3-x_Py_Py^3+x_P^2y_P^2x^2y^2\\ &= xy-(x^3+y^3)x_Py_P+x_P^2y_P^2x^2y^2\\ &= xy-(-1+dxy)x_Py_P+x_P^2y_P^2x^2y^2\\ &= xy+x_Py_P-dx_Py_Pxy+x_P^2y_P^2x^2y^2\\ &= x_Py_P+xy-dx_Py_Pxy+x_P^2y_P^2x^2y^2\end{aligned}$$

so that

$$(y-x_Py_Px^2)(x-x_Py_Py^2) = (y_P-x_P^2xy)(x_P-y_P^2xy) = . \tag{5}$$

$xy+x_Py_P-dx_Py_Pxy+x_P^2y_P^2x^2y^2$ Therefore
$\frac{y_P-x_P^2xy}{x_Px^2-y_P^2y}*\frac{x_P-y_P^2xy}{y_Px^2-x_P^2y} =$

$$= \frac{(y-x_Py_Px^2)(x-x_Py_Py^2)}{(x-x_Py_Py^2)(xy-x_Py_P)}$$
$$= \frac{y-x_Py_Px^2}{xy-x_Py_P}.$$

So we can write equality (2) as

$$g(x,y) = (y\prod_{Q\in S}\frac{x_Q^2y^2-x}{x_Qx^2-x_Q^2y}\cdot\prod_{P\in R_-}\frac{x-x_Py_Py^2}{xy-x_Py_P}, x\prod_{Q\in S}\frac{1-x_Qxy}{x^2-x_Qy}\cdot\prod_{P\in R_-}\frac{y-x_Py_Px^2}{xy-x_Py_P})$$

which completes the proof.

Theorem 5 *Let G be a subgroup of H_d of finite order ℓ non-divisible by 3 then the map*

$$g(x,y) = (y\prod_{Q\in S}\frac{x_Q^2y^2-x}{x_Qx^2-x_Q^2y}\cdot\prod_{P\in R_-}\frac{x-x_Py_Py^2}{xy-x_Py_P}, x\prod_{Q\in S}\frac{1-x_Qxy}{x^2-x_Qy}\cdot\prod_{P\in R_-}\frac{y-x_Py_Px^2}{xy-x_Py_P}) \tag{6}$$

defined in Lemma 2 is an isogeny of kernel G from H_d to $H_{d'}$ with $d' = \prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)\cdot(d(1+2r-2s)+6\sum_{Q\in S}x_Q)-6S_{r,r-1}(x_{P_1}y_{P_1},\ldots,x_{P_r}y_{P_r})\cdot\prod_{Q\in S}x_Q$

Proof .

1. It is easy to see that g is invariant by translation on elements of G. Furthermore

$$\begin{aligned} g(1:-1:0) &= (\prod_{Q\in G} Y_Q : \prod_{Q\in G} X_Q : \prod_{Q\in G} Z_Q) \\ &= (\prod_{Q\in G^*} Y_Q : -\prod_{Q\in G^*} X_Q : 0) \\ &= (1:-1:0) \end{aligned}$$

Because $\prod_{Q\in G^*} Y_Q = \prod_{Q\in G^*} X_Q$ since G is a subgroup and $Y_Q = X_{-Q}$. So $G \subseteq ker(g)$. We now show that $G = ker(g)$

(a) For this we first compute the image of $(-1,0)$ and $(1:-1:0)$

$$\begin{aligned} g(-1,0) &= (\prod_{P\in G} Y_{(-1,0)+P} : \prod_{P\in G} X_{(-1,0)+P} : \prod_{P\in G} Z_{(-1,0)+P}) \\ &= (0 * \prod_{P\in G^*} Y_{(-1,0)+P} : -\prod_{P\in G^*} X_{(-1,0)+P} : \prod_{P\in G^*} Z_{(-1,0)+P}) \\ &= (0 * \prod_{P\in G^*} Z_P : -\prod_{P\in G^*} Y_P : \prod_{P\in G^*} X_P) \\ &= (0, -\prod_{P\in G^*} Y_P/X_P), \quad \prod_{P\in G^*} X_P = \prod_{P\in G^*} Y_P \\ &= (0,-1) \end{aligned}$$

$$\begin{aligned} g(1:-j:0) &= (\prod_{P\in G} Y_{(1:-j:0)+P} : \prod_{P\in G} X_{(1:-j:0)+P} : \prod_{P\in G} Z_{(1:-j:0)+P}) \\ &= (\prod_{P\in G} j^2 Y_P : \prod_{P\in G} jX_P : \prod_{P\in G} Z_P) \\ &= (-j^2 \prod_{P\in G^*} j^2 Y_P : j \prod_{P\in G^*} jX_P : 0 * \prod_{P\in G^*} Z_P) \\ &= (-j^{2\#G} \prod_{P\in G^*} Y_P : j^{\#G} \prod_{P\in G^*} X_P : 0) \\ &= (-j^{2\#G} : j^{\#G} : 0) \\ &= \pm(1:-j:0) \quad \textit{since} \quad \#G \quad \textit{is} \quad \textit{not} \quad \textit{divisible} \quad \textit{by} \quad 3 \end{aligned}$$

$g(1:-j:0) = (1:-j:0)$ if $\#G = 2 \bmod 3$ and $g(1:-j:0) = -(1:-j:0)$ if $\#G = 1 \bmod 3$. So $(-1,0)$ and $(1:-j:0) \notin ker(g)$ ($ker(g)$ does not contain a point at infinity).

(b) Let $P_0(x_0,y_0)$ such that $g(P_0) = (1:-1:0)$ Since the image of P_0 is at infinity then P_0 is a zero of denominator of a component of g.
   - If (x_0,y_0) is an zero of $xy - x_P y_P$ then $(x_0,y_0) = \pm(x_P,y_P)$, $\pm(jx_P, j^2 y_P)$ or $\pm(j^2 x_P, jy_P)$ (from Bezout's theorem $xy - x_P y_P$ has six intersection points with H_d). g is an isogeny and $(1:-j:0) \notin ker(g)$ so $(x_0,y_0) = \pm(x_P,y_P)$ since $(jx_P, j^2 y_P) = (x_P,y_P) + (1:-j:0)$ and $(j^2 x_P, jy_P) = (x_P,y_P) + (1:-j^2:0)$.
   - If (x_0,y_0) is an zero of $x^2 - x_Q y$ then $(x_0,y_0) = (x_Q,x_Q)$, $\pm(jx_Q, j^2 x_Q)$, $(1, 1/x_Q)$, $(j, j^2/x_Q)$ or $(j^2, j/x_Q)$(from Bezout's theorem $x^2 - x_Q y$ has six intersection points with H_d).g is an isogeny and $(0,-1)$, $(1:-j:0) \notin ker(g)$ so $(x_0,y_0) = (x_Q,x_Q)$ since $(jx_Q, j^2 x_Q) = (x_Q,y_Q) + (1:-j:0)$ $(1,1/x_Q) = (x_Q,y_Q) + (-1,0)$, $(j^2, j/x_Q) = (x_Q,y_Q) + (-1,0) + (1:-j^2:0)$ and $(j, j^2/x_Q) = (x_Q,y_Q) + (-1,0) + (1:-j:0)$

2. We now show that $H(x,y) = g_x^3 + g_y^3 + 1 - d'g_x g_y$ has a pole of order two at neutral point $(1:-1:0)$ The uniformizer of the curve the neutral point is $t = \frac{Z}{3j^2X+3jY+dZ}$. The function Z has three zero $(1:-1:0), (1:-j:0)$ *and* $(1:-j^2:0)$. Also $3j^2X + 3jY + dZ$ has three zero $(1:-j:0)$ and two affine points. So t has exactly two zero $(1:-1:0)$ and $(1:-j^2:0)$. We have show that $g(1:-1:0) = (1:-1:0)$ and $g(1:-j^2:0) = \pm(1:-j^2:0)$ up to composition by the automorphism $(X:Y:Z) \mapsto (Y:X:Z)$ we can suppose that $g(1:-j^2:0) = (1:-j^2:0)$. In this case $(1:-1:0)$ and $(1:-j^2:0)$ are preserved by the coordinates map. Furthermore $(1:-1:0)$ and $(1:-j^2:0)$ are the only zero of $t = \frac{Z}{3j^2X+3jY+dZ}$. That is the same to co-domain curve $H_{d'}$ for which $t' = \frac{Z}{3j^2X+3jY+d'Z}$ has only two zeros $(1:-1:0)$ and $(1:-j^2:0)$. We now prove that the two points are nonsingular. The equation of the curve $H(X:Y:Z) =$
$\frac{Y^3}{Z^3}\prod_{Q\in S}\frac{(x_Q^2Y^2-XZ)^3}{(x_QX^2-x_Q^2YZ)^3}\cdot\prod_{P\in R_-}\frac{(XZ-x_Py_PY^2)^3}{(XY-x_Py_PZ^2)^3}+$
$\frac{X^3}{Z^3}\prod_{Q\in S}\frac{(Z^2-x_QXY)^3}{(X^2-x_QYZ)^3}\cdot\prod_{P\in R_-}\frac{(YZ-x_Py_PX^2)^3}{(XY-x_Py_PZ^2)^3}+1$
$-d'\frac{XY}{Z^2}\prod_{Q\in S}\frac{(x_Q^2Y^2-XZ)(Z^2-x_QXY)}{x_Q(X^2-x_QYZ)^2}\cdot\prod_{P\in R_-}\frac{(XZ-x_Py_PY^2)(YZ-x_Py_PX^2)}{(XY-x_Py_PZ^2)^2}$
shows, after reduction to the same denominator, the numerator
$N = Y^3\prod_{Q\in S}\left((x_Q^2Y^2-XZ)^3/x_Q^3\right)\cdot\prod_{P\in R_-}(XZ-x_Py_PY^2)^3 + X^3\prod_{Q\in S}(Z^2-x_QXY)^3\cdot\prod_{P\in R_-}(YZ-x_Py_PX^2)^3 + Z^3\prod_{Q\in S}(X^2-x_QYZ)^3\cdot\prod_{P\in R_-}(XY-x_Py_PZ^2)^3 - d'XYZ\prod_{Q\in S}\Big((Z^2-x_QXY)(X^2-x_QYZ)(x_Q^2Y^2-XZ)/x_Q\Big)\cdot$
$\prod_{P\in R_-}\big((XZ-x_Py_PY^2)(YZ-x_Py_PX^2)(XY-x_Py_PZ^2)\big)$ and the denominator
$D = Z^3\prod_{Q\in S}(X^2-x_QYZ)^3\cdot\prod_{P\in R_-}(XY-x_Py_PZ^2)^3$ We will show that $(1:-1:0)$ and $(1:-j^2:0)$ are the simple zero of N and the zero of order 3 of D (so the poles of order 2 of $H(X:Y:Z)$) . To show that the points $(1:-1:0)$ and $(1:-j^2:0)$ are zero of order 3 of D we will use affine coordinates in the plane $((y,z))$ in which $(1:-1:0)$ and $(1:-j^2:0)$ become $(-1,0)$ and $(-j^2,0)$ and $D = z^3\prod_{Q\in S}(1-x_Qyz)^3\prod_{P\in R_-}(y-x_Py_Pz^2)^3$
To bring back the point $(1:-1:0)$ (resp $(1:-j^2:0)$) to the origin $(0,0)$, we use the invertible affine coordinate transformation $(y',z') = (y-1,z)$ (resp $(y',z') = (y-j^2,z)$)
$D = z'^3\prod_{Q\in S}(1-x_Qz'-x_Qy'z')^3\cdot\prod_{P\in R_-}(y'+1-x_Py_Pz^2)^3$
$\Big($resp. $D = z'^3\prod_{Q\in S}(1-x_Qj^2z'-x_Qy'z')^3\cdot\prod_{P\in R_-}(y'+j^2-x_Py_Pz'^2)^3\Big)$. We see that the smallest homogeneous part of D has degree 3. So $(-1,0)$ and $(-j^2,0)$ are zero of order 3 of D. It easy to see that $(1:-1:0)$ and $(1:-j^2:0)$ are the zero of N. For show that $(1:-1:0)$ and $(1:-j^2:0)$ are simple zero we show that $\frac{\partial N}{\partial Y}(1:-1:0)\neq 0$ and $\frac{\partial N}{\partial Y}(1:-j^2:0)\neq 0$.
$\frac{\partial N}{\partial Y} = 3Y^2\prod_{Q\in S}\left((x_Q^2Y^2-XZ)^3/x_Q^3\right)\cdot\prod_{P\in R_-}(XZ-x_Py_PY^2)^3 + Y^3\prod_{P\in R_-}$
$(XZ-x_Py_PY^2)^3\cdot\sum_{Q_0}\left(6x_{Q_0}^2Y(x_{Q_0}^2Y^2-XZ)^2/x_{Q_0}^3\prod_{Q\neq Q_0}(x_Q^2Y^2-XZ)^3/x_Q^3\right)+Y^3\prod_{Q\in S}\left((x_Q^2Y^2-XZ)^3/x_Q^3\right)\cdot$

$\sum_{P_0\in R_-}\left(-6x_{P_0}y_{P_0}Y(XZ-x_{P_0}y_{P_0}Y^2)^2\prod_{P\neq P_0}(XZ-x_Py_PY^2)^3\right)+X^3\prod_{Q\in S}(Z^2-x_QXY)^3\cdot$
$\sum_{P_0\in R_-}\left(3Z(YZ-x_{P_0}y_{P_0}X^2)^2\prod_{P\neq P_0}(YZ-x_Py_PX^2)^3\right)+X^3\prod_{P\in R_-}(YZ-x_Py_PX^2)^3\cdot\sum_{Q_0\in S}\left(-3x_{Q_0}X(Z^2-x_{Q_0}XY)^2\cdot\prod_{Q\neq Q_0}(Z^2-x_QXY)^3\right)+$
$(Z^3\prod_{Q\in S}(X^2-x_QYZ)^3\cdot\prod_{P\in R_-}(XY-x_Py_PZ^2)^3)'_Y -$
$d'XYZ\prod_{Q\in S}\left((Z^2-x_QXY)(X^2-x_QYZ)(x_Q^2Y^2-XZ)/x_Q\right)\cdot$
$\prod_{P\in R_-}\big((XZ-x_Py_PY^2)(YZ-x_Py_PX^2)(XY-x_Py_PZ^2)\big))'_Y$
Therefore,
$\frac{\partial N}{\partial Y}(1:-1:0) = 3\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3) -$
$\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(-6x_{Q_0}^3\prod_{Q\neq Q_0}x_Q^3\right) -$

$\prod_{Q\in S} x_Q^3 \cdot \sum_{P_0}\left(6x_{P_0}^3 y_{P_0}^3 \prod_{P\neq P_0}(-x_P^3y_P^3)\right)+0$
$+\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(-3x_{Q_0}^3\prod_{Q\neq Q_0}x_Q^3\right)$
$\frac{\partial N}{\partial Y}(1:-1:0)=3\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3)+6\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(\prod_Q x_Q^3\right)+6\prod_{Q\in S}x_Q^3\cdot$
$\sum_{P_0}\left(\prod_P(-x_P^3y_P^3)\right)+0-3\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(\prod_Q x_Q^3\right).$
then
$\frac{\partial N}{\partial Y}(1:-1:0)=(3+6s+6r-3s)\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3)$
$\frac{\partial N}{\partial Y}(1:-1:0)=(3+3s+6r)\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3)$ and
$\frac{\partial N}{\partial Y}(1:-j^2:0)=3j\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3)-$
$\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(-6jx_{Q_0}^3\prod_{Q\neq Q_0}x_Q^3\right)-$
$\prod_{Q\in S}x_Q^3\cdot\sum_{P_0}\left(6jx_{P_0}^3y_{P_0}^3\prod_{P\neq P_0}(-x_P^3y_P^3)\right)+0$
$+\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(-3jx_{Q_0}^3\prod_{Q\neq Q_0}x_Q^3\right)$
$\frac{\partial N}{\partial Y}(1:-j^2:0)=3j\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3)+6j\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(\prod_Q x_Q^3\right)+$
$6j\prod_{Q\in S}x_Q^3\cdot\sum_{P_0}\left(\prod_P(-x_P^3y_P^3)\right)+0-3j\prod_{P\in R_-}(-x_P^3y_P^3)\cdot\sum_{Q_0}\left(\prod_Q x_Q^3\right).$
Then
$\frac{\partial N}{\partial Y}(1:-j^2:0)=(3j+6sj+6rj-3sj)\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3)$ and
$\frac{\partial N}{\partial Y}(1:-j^2:0)=(3+3s+6r)j\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(-x_P^3y_P^3)$. So $(1:-1:0)$ and $(1:-j^2:0)$ are the poles of other 2 of $H(X:Y:Z)$.

3. To develop $g_x^3+g_y^3+1-d'g_xg_y$ around of neutral point, we start to develop the function x and y To express xy in term of $t=\frac{1}{3j^2x+3jy+d}$ we will use the identity $a^3+b^3=(a+b)^3-3ab(a+b)$. We have

$$\begin{aligned}-1+dxy &= x^3+y^3\\ &= (j^2x)^3+(jy)^3\\ &= (j^2x+jy)^3-3xy(j^2x+jy)\\ &= (\frac{-dt+1}{3t})^3-3xy(\frac{-dt+1}{3t})\end{aligned}$$

as $\quad j^2x+jy=\frac{-dt+1}{3t}$ since $t=\frac{1}{3j^2x+3jy+d}$. Therefore
$xy=\frac{(\frac{-dt+1}{3t})^3+1}{d+\frac{-dt+1}{t}}=\frac{(d^3-27)t^3-3d^2t^2+3dt-1}{-27t^2}=\frac{\frac{1}{27}}{t^2}+\frac{-\frac{1}{9}d}{t}+\frac{1}{9}d^2+(-\frac{1}{27}d^3+1)t.$
Now $x=\frac{X}{Z}=\frac{X}{3j^2X+3jY+dZ}*\frac{3j^2X+3jY+dZ}{Z}$ and $y=\frac{Y}{Z}=\frac{Y}{3j^2X+3jY+dZ}*\frac{3j^2X+3jY+dZ}{Z}$. Hence x and y have a simple pole at neutral point and the values of $\frac{X}{3j^2X+3jY+dZ}$ and $\frac{Y}{3j^2X+3jY+dZ}$ at $(1:-1:0)$ are respectively $2j/9+1/9$ and $-2j/9-1/9$. Let $x=\frac{2j/9+1/9}{t}+a_0+O(t)$ and $y=-\frac{2j/9+1/9}{t}+b_0+O(t)$. We now want to compute a_0 *and* b_0 . A sage script available in [21, developInf.ipynb (first cell)] enables to compute $x*$

$\left(-jx-\frac{dj^2}{3}+\frac{j^2}{3t}\right)$,$y*\left(-j^2y-\frac{dj}{3}+\frac{j}{3t}\right)$ and develop x^3 and y^3 to get

$$\begin{aligned}
xy &= x*\left(-jx-\frac{dj^2}{3}+\frac{j^2}{3t}\right)\\
&= \left(\frac{2j/9+1/9}{t}+a_0+O(t)\right)*\left(\frac{-\frac{2}{9}j-\frac{1}{9}}{t}+\left(\frac{1}{3}j+\frac{1}{3}\right)d-ja_0+O(t)\right)\\
&= \frac{\frac{1}{27}}{t^2}+\frac{\left(\frac{1}{27}j-\frac{1}{27}\right)d+\left(-\frac{1}{9}j+\frac{1}{9}\right)a_0}{t}+O(1)
\end{aligned}$$

so that $a_0=\frac{-d/9-\left(\frac{1}{27}j-\frac{1}{27}\right)d}{\left(-\frac{1}{9}j+\frac{1}{9}\right)}=\left(-\frac{1}{3}j-\frac{1}{3}\right)d$. Similarly,

$$\begin{aligned}
xy &= y*\left(-j^2y-\frac{dj}{3}+\frac{j}{3t}\right)\\
&= \left(-\frac{2j/9+1/9}{t}+b_0+O(t)\right)*\left(\frac{\frac{2}{9}j+\frac{1}{9}}{t}-\frac{1}{3}jd+(j+1)b_0+O(t)\right)\\
&= \frac{\frac{1}{27}}{t^2}+\frac{\left(-\frac{1}{27}j-\frac{2}{27}\right)d+\left(\frac{1}{9}j+\frac{2}{9}\right)b_0}{t}+O(1)
\end{aligned}$$

so that $b_0=\frac{-d/9-\left(-\frac{1}{27}j-\frac{2}{27}\right)d}{\left(\frac{1}{9}j+\frac{2}{9}\right)}=\frac{1}{3}jd$

4. Development of $g_x^3+g_y^3+1-d'g_xg_y$ around of neutral point and value of d' We have

$$x=\frac{2j/9+1/9}{t}+\left(-\frac{1}{3}j-\frac{1}{3}\right)d+O(t)\quad and \quad y=-\frac{2j/9+1/9}{t}+\frac{1}{3}jd+O(t)$$

so that

$$x^3=\frac{-\frac{2}{243}j-\frac{1}{243}}{t^3}+\frac{\left(\frac{1}{27}j+\frac{1}{27}\right)d}{t^2}+O(t^{-1})\quad and \quad y^3=\frac{\frac{2}{243}j+\frac{1}{243}}{t^3}+\frac{-\frac{1}{27}jd}{t^2}+O(t^{-1})$$

– Let $Q\in S$ A sage script available in [21, developInf.ipynb (second cell)] enables to develop $\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}$, $\left(\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}\right)^3$, $\frac{1-x_Qxy}{x^2-x_Qy}$, $\left(\frac{1-x_Qxy}{x^2-x_Qy}\right)^3$,and $\frac{1-x_Qxy}{x^2-x_Qy}\cdot\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}$ around neutral point $(1:-1:0)$).
$\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}=x_Q+\left(\frac{\left(\frac{4}{19683}j+\frac{2}{19683}\right)dx_Q^2+\left(-\frac{2}{6561}j-\frac{1}{6561}\right)x_Q^3-\frac{2}{6561}j-\frac{1}{6561}}{-\frac{1}{19683}x_Q}\right)t+O(t^2)$
$\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}=x_Q+\left(\frac{\left(\frac{1}{19683}j+\frac{1}{39366}\right)dx_Q^2-\frac{1}{6561}j-\frac{1}{13122}}{-\frac{1}{19683}x_Q}\right)t+O(t^2)\quad since \quad ,x_Q^3=(-1+dx_Q^2)/2$

we use the fact that $2x_Q^3+1=dx_Q^2\Rightarrow 1/x_Q=-2x_Q^2+dx_Q$
$\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}=$
$=x_Q+\left(\left(-j-\frac{1}{2}\right)d^2x_Q^3+(2j+1)dx_Q^4+\left(3j+\frac{3}{2}\right)dx_Q+(-6j-3)x_Q^2\right)t+O(t^2)$
$=x_Q+(2j+1)\left(dx_Q-3x_Q^2\right)t+O(t^2)\quad since \quad x_Q^3=\frac{-1+dx_Q^2}{2}$ Therefore

$$\left(\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}\right)^3=x_Q^3+(6j+3)\left(dx_Q^3-3x_Q^4\right)t+O(t^2)$$

$\frac{1-x_Qxy}{x^2-x_Qy} = x_Q - (2j+1)\left(dx_Q - 3x_Q^2\right)t + O(t^2)$
so $(\frac{1-x_Qxy}{x^2-x_Qy})^3 = x_Q^3 - (6j+3)\left(dx_Q^3 - 3x_Q^4\right)t + O(t^2)$ and

$$\frac{1-x_Qxy}{x^2-x_Qy} * \frac{x_Qy^2-x}{x_Qx^2-x_Q^2y} = x_Q^2 + O(t^2)$$

we will use the following equality

$$\prod_{i\in I}\left(a_i + b_it + O(t^2)\right) = \prod_{i\in I} a_i + \sum_{i_0\in I}\left(b_{i_0}\prod_{i\neq i_0} a_i\right)t + O(t^2)$$

Now we have $\prod_{Q\in S}\left(\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y}\right)^3$

$$\begin{aligned}
&= \prod_{Q\in S} x_Q^3 + (6j+3)\sum_{Q_0\in S}\left((dx_{Q_0}^3 - 3x_{Q_0}^4)\prod_{Q\neq Q_0} x_Q^3\right)t + O(t^2)\\
&= \prod_{Q\in S} x_Q^3 + (6j+3)\sum_{Q_0\in S}\left(dx_{Q_0}^3\prod_{Q\neq Q_0} x_Q^3 - 3x_{Q_0}^4\prod_{Q\neq Q_0} x_Q^3\right)t + O(t^2)\\
&= \prod_{Q\in S} x_Q^3 + (6j+3)\sum_{Q_0\in S}\left(d\prod_Q x_Q^3 - 3x_{Q_0}\prod_Q x_Q^3\right)t + O(t^2)\\
&= \prod_{Q\in S} x_Q^3 + (6j+3)\prod_Q x_Q^3 \cdot \sum_{Q\in S}(d-3x_Q)t + O(t^2)
\end{aligned}$$

$\prod_{Q\in S}\left(\frac{1-x_Qxy}{x^2-x_Qy}\right)^3$

$$\begin{aligned}
&= \prod_{Q\in S} x_Q^3 - (6j+3)\sum_{Q_0\in S}\left((dx_{Q_0}^3 - 3x_{Q_0}^4)\prod_{Q\neq Q_0} x_Q^3\right)t + O(t^2)\\
&= \prod_{Q\in S} x_Q^3 - (6j+3)\sum_{Q_0\in S}\left(dx_{Q_0}^3\prod_{Q\neq Q_0} x_Q^3 - 3x_{Q_0}^4\prod_{Q\neq Q_0} x_Q^3\right)t + O(t^2)\\
&= \prod_{Q\in S} x_Q^3 - (6j+3)\sum_{Q_0\in S}\left(d\prod_Q x_Q^3 - 3x_{Q_0}\prod_Q x_Q^3\right)t + O(t^2)\\
&= \prod_{Q\in S} x_Q^3 - (6j+3)\prod_Q x_Q^3 \cdot \sum_{Q\in S}(d-3x_Q)t + O(t^2)
\end{aligned}$$

$$\prod_{Q\in S}\left(\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y} * \frac{1-x_Qxy}{x^2-x_Qy}\right) = \prod_{Q\in S} x_Q^2 + O(t^2)$$

- Let $P \in R$
$\frac{-x_P*y_P*y^2+x}{xy-x_Py_P}$(a sage script available in [21, developInf.ipynb (third cell)] enables to compute the development of $\frac{-x_P*y_P*y^2+x}{xy-x_Py_P}$, $\left(\frac{-x_P*y_P*y^2+x}{xy-x_Py_P}\right)^3$, $\frac{-x_P*y_P*x^2+y}{xy-x_Py_P}$,$\left(\frac{-x_P*y_P*x^2+y}{xy-x_Py_P}\right)^3$,and $\frac{-x_P*y_P*y^2+x}{xy-x_Py_P} \cdot \frac{-x_P*y_P*x^2+y}{xy-x_Py_P}$ around neutral point (1 :

$-1:0)$). We have
$\frac{-x_P*y_P*y^2+x}{xy-x_Py_P} = x_Py_P - (2j+1)(dx_Py_P-3)t + O(t^2)$
so that $(\frac{-x_P*y_P*y^2+x}{xy-x_Py_P})^3 = x_P^3y_P^3 - (6j+3)\left(dx_P^3y_P^3 - 3x_P^2y_P^2\right)t + O(t^2)$ Also

$$\frac{-x_P*y_P*x^2+y}{xy-x_Py_P} = x_Py_P + (2j+1)(dx_Py_P-3)t + O(t^2)$$

so that

$$(\frac{-x_P*y_P*x^2+y}{xy-x_Py_P})^3 = x_P^3y_P^3 + (6j+3)\left(dx_P^3y_P^3 - 3x_P^2y_P^2\right)t + O(t^2)$$

and

$$\frac{-x_P*y_P*x^2+y}{xy-x_Py_P} * \frac{-x_P*y_P*y^2+x}{xy-x_Py_P} = x_P^2y_P^2 + O(t^2)$$

$\prod_{P\in R_-}(\frac{-x_P*y_P*y^2+x}{xy-x_Py_P})^3 =$
$= \prod_{P\in R_-}(x_P^3y_P^3) - (6j+3)\sum_{P_0\in R_-}\left((dx_{P_0}^3y_{P_0}^3 - 3x_{P_0}^2y_{P_0}^2)\prod_{P\neq P_0}(x_P^3y_P^3)\right)t + O(t^2)$
$= \prod_{P\in R_-}(x_P^3y_P^3) -$
$(6j+3)\sum_{P_0\in R_-}\left(dx_{P_0}^3y_{P_0}^3\prod_{P\neq P_0}(x_P^3y_P^3) - 3x_{P_0}^2y_{P_0}^2\prod_{P\neq P_0}(x_P^3y_P^3)\right)t + O(t^2)$
$= \prod_{P\in R_-}(x_P^3y_P^3) -$
$(6j+3)\sum_{P_0\in R_-}\left(d\prod_{P\in R_-}(x_P^3y_P^3) - 3\prod_{P\in R_-}(x_P^2y_P^2)\cdot\prod_{P\neq P_0}(x_Py_P)\right)t + O(t^2)$
$= \prod_{P\in R_-}(x_P^3y_P^3) -$
$(6j+3)\left(rd\prod_{P\in R_-}x_P^3y_P^3 - 3\prod_{P\in R_-}(x_P^2y_P^2)\cdot\sum_{P\in R_-}\left(\prod_{P\neq P_0}(x_Py_P)\right)\right)t + O(t^2)$
$= \prod_{P\in R_-}(x_P^3y_P^3) -$
$(6j+3)\left(rd\prod_{P\in R_-}(x_P^3y_P^3) - 3\prod_{P\in R_-}(x_P^2y_P^2)\cdot S_{r,r-1}(x_{P_1}y_{P_1},\ldots,x_{P_r}y_{P_r})\right)t + O(t^2)$
$\prod_{P\in R_-}(\frac{-x_P*y_P*x^2+y}{xy-x_Py_P})^3 =$
$= \prod_{P\in R_-}(x_P^3y_P^3) +$
$(6j+3)\sum_{P_0\in R_-}\left((dx_{P_0}^3y_{P_0}^3 - 3x_{P_0}^2y_{P_0}^2)\prod_{P\neq P_0}(x_P^3y_P^3)\right)t + O(t^2)$
$= \prod_{P\in R_-}(x_P^3y_P^3) +$
$(6j+3)\left(rd\prod_{P\in R_-}(x_P^3y_P^3) - 3\prod_{P\in R_-}(x_P^2y_P^2)\cdot S_{r,r-1}(x_Py_P,\ldots,x_Py_P)\right)t + O(t^2)$
$\prod_{P\in R_-}(\frac{-x_P*y_P*x^2+y}{xy-x_Py_P} * \frac{-x_P*y_P*y^2+x}{xy-x_Py_P}) = \prod_{P\in R_-}(x_P^2y_P^2) + O(t^2)$

A sage script available in [21, developInf.ipynb (fourth cell)] enables to develop $x^3 * (a+bt+O(t^2))*(e+ft+O(t^2))$, $y^3*(a+bt+O(t^2))*(e+ft+O(t^2))$ and $xy*(a+bt+O(t^2))*(e+ft+O(t^2))$. We use the result here for compute g_x^3,g_y^3 and g_xg_y).

$g_x^3 = y^3\prod_{Q\in S}(\frac{x_Qy^2-x}{x_Qx^2-x_Q^2y})^3 \cdot \prod_{P\in R_-}(\frac{-x_P*y_P*y^2+x}{xy-x_Py_P})^3 = \frac{(2j/243+1/243)\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3)}{t^3} +$
$\frac{-\frac{jd}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3) + \frac{1}{27}\left(rd\prod_{P\in R_-}(x_P^3y_P^3) - 3\prod_{P\in R_-}(x_P^2y_P^2)\cdot S_{r-1}(x_{P_1}y_{P_1},\ldots,x_{P_r}y_{P_r})\right)\cdot\prod_{Q\in S}x_Q^3}{t^2}$
$- \frac{\frac{1}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3)\cdot\sum_{Q\in S}(d-3x_Q)}{t^2} + O(t^{-1})$.
Also
$g_y^3 = x^3\prod_{Q\in S}(\frac{1-x_Qxy}{x^2-x_Qy})^3 \cdot \prod_{P\in R_-}(\frac{-x_P*y_P*x^2+y}{xy-x_Py_P})^3 = \frac{-(2j/243+1/243)\prod_{i=1}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3)}{t^3} +$
$\frac{\frac{(j+1)d}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3) + \frac{1}{27}\left(rd\prod_{P\in R_-}x_P^3y_P^3 - 3\prod_{P\in R_-}(x_P^2y_P^2)\cdot S_{r,r-1}(x_{P_1}y_{P_1},\ldots,x_{P_r}y_{P_r})\right)\prod_{Q\in S}x_Q^3}{t^2}$
$- \frac{\frac{1}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{k=1}(x_P^3y_P^3)\cdot\sum_{Q\in S}(d-3x_Q)}{t^2} + O(t^{-1})$. Finally
$g_xg_y = xy\prod_{Q\in S}(\frac{1-x_Qxy}{x^2-x_Qy} * \frac{x_Qy^2-x}{x_Qx^2-x_Q^2y})\prod_{P\in R_-}(\frac{-x_P*y_P*x^2+y}{xy-x_Py_P} * \frac{-x_P*y_P*y^2+x}{xy-x_Py_P}) = \frac{\frac{1}{27}\prod_{i=1}x_Q^2\cdot\prod_{k=1}(x_P^2y_P^2)}{t^2} + O(t^{-1})$.

Therefore $g_x^3+g_y^3+1-d'g_xg_y=$
$=\frac{\frac{d}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3)}{t^2}$
$+\frac{\frac{2}{27}\left(rd\prod_{P\in R_-}(x_P^3y_P^3)-3\prod_{P\in R_-}(x_P^2y_P^2)\cdot S_{r-1}(x_{P_1}y_{P_1},\dots,x_{P_r}y_{P_r})\right)\prod_{Q\in S}x_Q^3}{t^2}-$
$\frac{\frac{2}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3)\cdot\sum_{Q\in S}(d-3x_Q)}{t^2}$
$-\frac{\frac{d'}{27}\prod_{Q\in S}x_Q^2\cdot\prod_{P\in R_-}(x_P^2y_P^2)}{t^2}+O(t^{-1})$
If we choose d' such that, $\frac{d}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3)+$
$\frac{2}{27}\left(rd\prod_{P\in R_-}x_P^3y_P^3-3\prod_{P\in R_-}(x_P^2y_P^2)\cdot S_{r,r-1}(x_{P_1}y_{P_1},\dots,x_{P_r}y_{P_r})\right)\cdot\prod_{Q\in S}x_Q^3-\frac{2}{27}\prod_{Q\in S}x_Q^3\cdot\prod_{P\in R_-}(x_P^3y_P^3)\cdot$
$\sum_{Q\in S}(d-3x_Q)-\frac{d'}{27}\prod_{Q\in S}x_Q^2\cdot\prod_{P\in R_-}(x_P^2y_P^2)=0$
then $g_x^3+g_y^3+1-d'g_xg_y=0$ since $g_x^3+g_y^3+1-d'g_xg_y$ is a pole of order 2 at $(1:-1:0)$ and $(1:-j^2:0)$.
$d'=d\prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)+2\left(rd\prod_{P\in R_-}(x_Py_P)-3S_{r,r-1}(x_{P_1}y_{P_1},\dots,x_{P_r}y_{P_r})\right)\cdot\prod_{Q\in S}x_Q$
$-2\prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)\cdot\sum_{Q\in S}(d-3x_Q)$
$d'=d\prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)+2rd\prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)$
$-6\prod_{Q\in S}x_Q\cdot S_{r,r-1}(x_{P_1}y_{P_1},\dots,x_{P_r}y_{P_r})$
$-2\prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)\cdot\sum_{Q\in S}(d-3x_Q)$
$d'=\prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)\left(d+2rd-2\sum_{Q\in S}(d-3x_Q)\right)-6\prod_{Q\in S}x_Q\cdot S_{r,r-1}(x_{P_1}y_{P_1},\dots,x_{P_r}y_{P_r})$
. Therefore $d'=\prod_{Q\in S}x_Q\cdot\prod_{P\in R_-}(x_Py_P)\left(d(1+2r-2s)+6\sum_{Q\in S}x_Q\right)-6S_{r,r-1}(x_{P_1}y_{P_1},\dots,x_{P_r}y_{P_r})\cdot\prod_{Q\in S}x_Q$.

The following Theorems 6 and 7 extend the previous result to isogenies over twisted and generalized Hessian curves.

Theorem 6 *Let $G=\{(1:-1:0)\}\cup\{(\gamma_j,\gamma_j)\}_{j=1}^s\cup\{\pm(\alpha_i,\beta_i)\}_{i=1}^r$ be a subgroup of the generalized Hessian curve $H_{c,d}$ of finite order ℓ non-divisible by 3. Then*

$$g(x,y)=(y\prod_{j=1}^{s}\frac{\gamma_j^2y^2-cx}{\gamma_jx^2-\gamma_j^2y}\cdot\prod_{i=1}^{r}\frac{-\alpha_i\beta_iy^2+cx}{xy-\alpha_i\beta_i},x\prod_{j=1}^{s}\frac{-\gamma_jxy+c}{x^2-\gamma_jy}\cdot\prod_{i=1}^{r}\frac{-\alpha_i\beta_ix^2+cy}{xy-\alpha_i\beta_i}) \qquad (7)$$

is an isogeny of kernel G from $H_{c,d}$ to $H_{c',d'}$ with $c'=c^n$ and $d'=\prod_{j=1}^s\gamma_j\cdot\prod_{i=1}^r(\alpha_i\beta_i)\cdot\left(d(1+2r-2s)+6\sum_{j=1}^s\gamma_j\right)-6cS_{r,r-1}(\alpha_1\beta_1,\dots,\alpha_r\beta_r)\cdot\prod_{j=1}^s\gamma_j$

Proof Using the isomorphism $f:H_{c,d}\longrightarrow H_{d/\sqrt[3]{c}}$, $f(x,y)=(\frac{x}{\sqrt[3]{c}},\frac{y}{\sqrt[3]{c}})$ (given in Subsection 2.2.1 between generalized Hessian curve and Hessian curve) the image of the subgroup $G=\{(1:-1:0)\}\cup\{(\gamma_j,\gamma_j)\}_{j=1}^s\cup\{\pm(\alpha_i,\beta_i)\}_{i=1}^r$ is the subgroup $G'=\{(1:-1:0)\}\cup\{(\frac{\gamma_j}{\sqrt[3]{c}},\frac{\gamma_j}{\sqrt[3]{c}})\}_{j=1}^s\cup\{\pm(\frac{\alpha_i}{\sqrt[3]{c}},\frac{\beta_i}{\sqrt[3]{c}})\}_{i=1}^r$. We apply Theorem 5 to have an isogeny $g:H_{d/\sqrt[3]{c}}\longrightarrow H_{d_1}$, $g(x,y)=(y\prod_{j=1}^s\frac{\gamma_j^2y^2-\sqrt[3]{c}^2x}{\gamma_j\sqrt[3]{c}x^2-\gamma_j^2y}\cdot\prod_{i=1}^r\frac{-\alpha_i\beta_iy^2+\sqrt[3]{c}^2x}{\sqrt[3]{c}^2xy-\alpha_i\beta_i},x\prod_{j=1}^s\frac{-\gamma_jxy+\sqrt[3]{c}}{\sqrt[3]{c}x^2-\gamma_jy}\cdot\prod_{i=1}^r\frac{-\alpha_i\beta_ix^2+\sqrt[3]{c}^2y}{\sqrt[3]{c}^2xy-\alpha_i\beta_i})$ with

$d_1=\prod_{j=1}^s\frac{\gamma_j}{\sqrt[3]{c}}\cdot\prod_{i=1}^r(\frac{\alpha_i\beta_i}{\sqrt[3]{c}^2})\cdot\left(\frac{d}{\sqrt[3]{c}}(1+2r-2s)+6\sum_{j=1}^s\frac{\gamma_j}{\sqrt[3]{c}}\right)-$
$6S_{r,r-1}(\frac{\alpha_1\beta_1}{\sqrt[3]{c}^2},\dots,\frac{\alpha_r\beta_r}{\sqrt[3]{c}^2})\cdot\prod_{j=1}^s\frac{\gamma_j}{\sqrt[3]{c}}$ which can be simplified from

$d_1=\frac{1}{\sqrt[3]{c}^s}\prod_{j=1}^s\gamma_j\cdot\frac{1}{\sqrt[3]{c}^{2r}}\prod_{i=1}^r(\alpha_i\beta_i)\cdot\left(\frac{d}{\sqrt[3]{c}}(1+2r-2s)+6\frac{1}{\sqrt[3]{c}}\sum_{j=1}^s\gamma_j\right)-$
$6\frac{1}{\sqrt[3]{c}^{2r-2}}S_{r,r-1}(\alpha_1\beta_1,\dots,\alpha_r\beta_r)\cdot\frac{1}{\sqrt[3]{c}^s}\prod_{j=1}^s\gamma_j$ to

$d_1=$
$\frac{1}{\sqrt[3]{c}^n}\left(\prod_{j=1}^s\gamma_j\cdot\prod_{i=1}^r(\alpha_i\beta_i)\cdot\left(d(1+2r-2s)+6\sum_{j=1}^s\gamma_j\right)-6cS_{r,r-1}(\alpha_1\beta_1,\dots,\alpha_r\beta_r)\cdot\prod_{j=1}^s\gamma_j\right)$.

We then apply the inverse transformation $f^{-1}: H_{d_1} \longrightarrow H_{c^n,d'}$ (given in Subsection 2.2.1 between generalized Hessian curve and Hessian curve) , $f^{-1}(x,y) = (\sqrt[3]{c^n}\cdot x, \sqrt[3]{c^n}\cdot y)$ where

$d' = \prod_{j=1}^{s}\gamma_j \cdot \prod_{i=1}^{r}(\alpha_i\beta_i)\cdot\Big(d(1+2r-2s)+6\sum_{j=1}^{s}\gamma_j\Big) - 6cS_{r,r-1}(\alpha_1\beta_1,...,\alpha_r\beta_r)\cdot\prod_{j=1}^{s}\gamma_j.$

$g\circ f(x,y) = (\frac{y}{\sqrt[3]{c}}\prod_{j=1}^{s}\frac{\gamma_j^2y^2-cx}{\sqrt[3]{c}(\gamma_jx^2-\gamma_j^2y)}\cdot\prod_{i=1}^{r}\frac{-\alpha_i\beta_iy^2+cx}{\sqrt[3]{c}^2(xy-\alpha_i\beta_i)}, \frac{x}{\sqrt[3]{c}}\prod_{j=1}^{s}\frac{-\gamma_jxy+c}{\sqrt[3]{c}(x^2-\gamma_jy)}\cdot\prod_{i=1}^{r}\frac{-\alpha_i\beta_ix^2+cy}{\sqrt[3]{c}^2(xy-\alpha_i\beta_i)})$

we get

$f^{-1}\circ g\circ f(x,y) = (y\prod_{j=1}^{s}\frac{\gamma_j^2y^2-cx}{\gamma_jx^2-\gamma_j^2y}\cdot\prod_{i=1}^{r}\frac{-\alpha_i\beta_iy^2+cx}{xy-\alpha_i\beta_i}, x\prod_{j=1}^{s}\frac{-\gamma_jxy+c}{x^2-\gamma_jy}\cdot\prod_{i=1}^{r}\frac{-\alpha_i\beta_ix^2+cy}{xy-\alpha_i\beta_i})$

Theorem 7 *Let $G = \{(0:-1:1)\}\cup\{(\gamma_j,1)\}_{j=1}^{s}\cup\{\pm(\alpha_i,\beta_i)\}_{i=1}^{r}$ be a subgroup of the twisted Hessian curve $\mathscr{H}_{a,d}$ of finite order ℓ non-divisible by 3. Then*

$$g(x,y) = (\frac{x}{y}\prod_{j=1}^{s}\frac{-xy+\gamma_j}{a\gamma_j^2x^2-y^2}\cdot\prod_{i=1}^{r}\frac{\alpha_i^2y-\beta_ix^2}{-\beta_iy^2+a\alpha_i^2x}, \frac{1}{y}\prod_{j=1}^{s}\frac{\gamma_jax^2-y}{a\gamma_j^2x^2-y^2}\cdot\prod_{i=1}^{r}\frac{a\alpha_i^2xy-\beta_i}{-\beta_iy^2+a\alpha_i^2x}) \quad (8)$$

is an isogeny of kernel G from $\mathscr{H}_{a,d}$ to $\mathscr{H}_{a',d'}$ with $a' = a^n$ and $d' = \prod_{j=1}^{s}\frac{1}{\gamma_j}\cdot\prod_{i=1}^{r}(\frac{\beta_i}{\alpha_i^2})\cdot\Big(d(1+2r-2s)+6\sum_{j=1}^{s}\frac{1}{\gamma_j}\Big) - 6aS_{r,r-1}(\frac{\beta_1}{\alpha_1^2},...,\frac{\beta_r}{\alpha_r^2})\cdot\prod_{j=1}^{s}\frac{1}{\gamma_j}$

Proof Using the isomorphism $f': \mathscr{H}_{a,d}\longrightarrow H_{a,d}$, $f(x,y) = (\frac{1}{x},\frac{y}{x})$ of Lemma 1 the image of the subgroup $G = \{(0:-1:1)\}\cup\{(\gamma_j,1)\}_{j=1}^{s}\cup\{\pm(\alpha_i,\beta_i)\}_{i=1}^{r}$ is the subgroup $G' = \{(1:-1:0)\}\cup\{(\frac{1}{\gamma_j},\frac{1}{\gamma_j})\}_{j=1}^{s}\cup\{\pm(\frac{1}{\alpha_i},\frac{\beta_i}{\alpha_i})\}_{i=1}^{r}$. We apply Theorem 6 to have an isogeny $g': H_{a,d}\longrightarrow H_{a^n,d'}$ defined by

$g'(x,y) = (y\prod_{j=1}^{s}\frac{-y^2+a\gamma_j^2}{\gamma_jx^2-y}\cdot\prod_{i=1}^{r}\frac{a\alpha_i^2x-\beta y^2}{\alpha_i^2xy-\beta_i}, x\prod_{j=1}^{s}\frac{a\gamma_j-xy}{\gamma_jx^2-y}\cdot\prod_{i=1}^{r}\frac{a\alpha_i^2y-\beta x^2}{\alpha_i^2xy-\beta_i})$ with

$d_1 = \prod_{j=1}^{s}\frac{1}{\gamma_j}\cdot\prod_{i=1}^{r}(\frac{\beta_i}{\alpha_i^2})\cdot\Big(d(1+2r-2s)+6\sum_{j=1}^{s}\frac{1}{\gamma_j}\Big) - 6aS_{r,r-1}(\frac{\beta_1}{\alpha_1^2},...,\frac{\beta_r}{\alpha_r^2})\cdot\prod_{j=1}^{s}\frac{1}{\gamma_j}.$

We then apply the inverse transformation given by Lemma 1 $f'^{-1}: H_{d_1}\longrightarrow\mathscr{H}_{a^n,d'}$, $f^{-1}(x,y) = (\frac{1}{x},\frac{y}{x})$. This leads to $g\circ f(x,y) = (\frac{y}{x}\prod_{j}^{s}\frac{a\gamma_j^2x^2-y^2}{-xy+\gamma_j}\cdot\prod_{i=1}^{r}\frac{-\beta_iy^2+a\alpha_i^2x}{\alpha_i^2y-\beta_ix^2}, \frac{1}{x}\prod_{j=1}^{s}\frac{\gamma_jax^2-y}{-xy+\gamma_j}\cdot\prod_{i=1}^{r}\frac{a\alpha_i^2xy-\beta_i}{\alpha_i^2y-\beta_ix^2})$ so that

$f'^{-1}\circ g'\circ f'(x,y) = (\frac{x}{y}\prod_{j}^{s}\frac{-xy+\gamma_j}{a\gamma_j^2x^2-y^2}\cdot\prod_{i=1}^{r}\frac{\alpha_i^2y-\beta_ix^2}{-\beta_iy^2+a\alpha_i^2x}, \frac{1}{y}\prod_{j=1}^{s}\frac{\gamma_jax^2-y}{a\gamma_j^2x^2-y^2}\cdot\prod_{i=1}^{r}\frac{a\alpha_i^2xy-\beta_i}{-\beta_iy^2+a\alpha_i^2x})$

5 Computational Cost of the Isogenies over Hessian Curves

In this section we examine the computational cost of the Hessian isogenies on input points and compare it to known results for Edward, Huff and Jacobi quartic isogenies [24] and [31].

5.1 Cost of Evaluation of Hessian Isogeny in Affine Coordinates

Let G an finite subgroup of H_d. We will use the notation of Theorem 5 where $g(x,y) = (y\prod_{Q\in S}\frac{x_Q^2y^2-x}{x_Qx^2-x_Q^2y}\cdot\prod_{P\in R_-}\frac{x-x_Py_Py^2}{xy-x_Py_P}, x\prod_{Q\in S}\frac{1-x_Qxy}{x^2-x_Qy}\cdot\prod_{P\in R_-}\frac{y-x_Py_Px^2}{xy-x_Py_P})$ Denote M, S and C the cost of a multiplication, squaring and multiplication by a constant in **K** respectively.

1. We first compute x^2, y^2 and xy at the cost of $M+2S$.
2. For each $P\in R_-$, we compute $y-x_Py_Px^2$ and $x-x_Py_Py^2$. This requires $2rC$. Similarly for each $Q\in S$ we compute $1-x_Qxy$, x^2-x_Qy and $\frac{1}{x_{Q_i}}(x_{Q_i}^2y^2-x)$ costing $4sC$.

3. The computation of $\prod_{P\in R_-}(y-x_Py_Px^2)$, $\prod_{P\in R_-}(xy-x_Py_P)$ and $\prod_{P\in R_-}(x-x_Py_Py^2)$ costs $3(r-1)M$. Similarly the computation of $\prod_{Q\in S}(x_Q^2y^2-x)$, $\prod_{Q\in S}(x^2-x_Qy)$ and $\prod_{Q\in S}(1-x_{Q_i}xy)$ costs $3(s-1)M$.
4. We compute $\prod_{P\in R_-}(xy-x_Py_P)*\prod_{Q\in S}(x^2-x_Qy)$ and the inverse $\frac{1}{\prod_{P\in R_-}(xy-x_Py_P)*\prod_{Q\in S}(x^2-x_Qy)}$ in $M+I$.
5. Finally the computation of $y\prod_{Q\in S}\left(\frac{1}{x_Q}(x_Q^2y^2-x)\right)*\prod_{P\in R_-}(x-x_Py_Py^2)\frac{1}{\prod_{P\in R_-}(xy-x_Py_P)*\prod_{Q\in S}(x^2-x_Qy)}$ and $x\prod_{Q\in S}(1-x_Qxy)*\prod_{P\in R_-}(y-x_Py_Px^2)\frac{1}{\prod_{P\in R_-}(xy-x_Py_P)*\prod_{Q\in S}(x^2-x_Qy)}$ costs $6M$.

The total total cost is then $(3s+3r+2)M+(4s+2r)C+2S+I$. In the particular case of 2-isogeny the cost is $5M+2S+4C+I$. In the case of subgroups of order not divisible by 2 and 3 the cost is $(3r+2)M+2rC+2S+I$.

5.2 Cost of Computing the Isogeny for Subgroup of Order 3 in Affine Coordinates

– First, second and third case of Theorem 2. In these cases $g(x,y)=(m\frac{x+x^2y+y^2}{xy},m\frac{y+y^2x+x^2}{xy})$ we first compute x^2,y^2 and xy at a cost of $2S+M$. Next we compute xy^2 and x^2y in $2M$. The computation of $\frac{1}{xy}$ costs $1I$. The computation of $(x+x^2y+y^2)(m\frac{1}{xy})$ and $(y+y^2x+x^2)(m\frac{1}{xy})$ requires $C+2M$. For the second and third case of Theorem 2 we add $4C$ for the computation of jx,jy,j^2x^2y and j^2y^2x in the second case (resp jx,jy,j^2x^2 and j^2y^2 in the third case). The total cost is $5M+2S+C+I$ for the first case and $5M+2S+5C+I$ for the second and third case.
– Fourth case of Theorem 2.
We have $g(x,y)=(m\frac{-jx^3+1-d(-1/3j+1/3)xy}{xy},m\frac{-jy^3+1-d(-1/3j+1/3)xy}{xy})$.
From the computation of x^3,y^3 one deduces $dxy=x^3+y^3+1$ and $xy=\frac{1}{d}(x^3+y^3+1)$ at the cost of $2S+2M+C$. The computation of $-jy^3$, $-jx^3$ and $(-1/3j+1/3)dxy$ requires $3C$. The computation of $\frac{1}{xy}$, $(-jy^3+1-d(-1/3j+1/3)xy)(m\frac{1}{xy})$ and $(-jy^3+1-d(-1/3j+1/3)xy)(m\frac{1}{xy})$ requires $C+2M$. The total cost is $4M+2S+4C+I$.

5.3 Cost of Computing the Isogeny in Projective Coordinates

$g(X:Y:Z)=(Y\prod_{Q\in S}\left(\frac{1}{x_Q}(x_Q^2Y^2-ZX)\right)\cdot\prod_{P\in R_-}(XZ-x_Py_PY^2):$
$X\prod_{Q\in S}(Z^2-x_QXY)\cdot\prod_{P\in R_-}(YZ-x_Py_PX^2):Z\prod_{P\in R_-}(XY-x_Py_PZ^2)\cdot\prod_{Q\in S}(X^2-x_QYZ))$

1. We first compute X^2,Y^2,Z^2,XZ,YZ and XY at a cost of $3M+3S$.
2. For each $P\in R_-$, the computation of $YZ-x_Py_PX^2$, $XZ-x_Py_PY^2$ and $XY-x_Py_PZ^2$ requires $3rC$. Also for each $Q\in S$ the computation of Z^2-x_QXY,X^2-x_QYZ and $\frac{1}{x_Q}(x_Q^2Y^2-XZ)$ costs $4sC$.
3. The computation of $\prod_{P\in R_-}(YZ-x_Py_PX^2)$, $\prod_{P\in R_-}(XY-x_Py_PZ^2)$ and $\prod_{P\in R_-}(XZ-x_Py_PY^2)$ costs $3(r-1)M$. Also, computing $\prod_{Q\in S}(x_Q^2Y^2-XZ)$, $\prod_{Q\in S}(X^2-x_QYZ)$ and $\prod_{Q\in S}(Z^2-x_QXY)$ requires $3(s-1)M$.
4. Finally the computation of $Y\prod_{Q\in S}\left(\frac{1}{x_Q}(x_{Q_i}^2Y^2-ZX)\right)\cdot\prod_{P\in R_-}(XZ-x_Py_PY^2)$, $X\prod_{Q\in S}(Z^2-x_{Q_i}XY)\cdot\prod_{P\in R_-}(Y-x_Py_PX^2)$ and $Z\prod_{P\in R_-}(XY-x_Py_PZ^2)\cdot\prod_{Q\in S}(X^2-x_QYZ)$ requires $6M$.

Table 1 Theoretic cost for computing isogenies of odd degree $\ell = 2s+1$ over elliptic curves

Curves	Cost in projective	Cost in affine
Edward [24]	$(3s+3)M+4S+3sC$	$(3s+1)M+2S+3sC+I$
Huff [24]	$(4s+3)M+3S+4sC$	$(4s-2)M+2S+2sC+2I$
Jacobi quartic [31]	$(4s+2)M+3S+(7s+4)C$	$(4s+2)M+3S+(7s+4)C+2I$
Twisted Hessian [7]	$(5s+3)M+4S+8sC$	$(5s+2)M+(s+2)S+7sC+I$
Twisted Hessian[27]	$(5s+5)M+3S+(9s)C$	$(5s+2)M+3S+9sC+I$
Hessian (This Work)	$(3s+3)M+3S+3sC$	$(3s+2)M+2S+2sC+I$

The total cost is then $(3s+3r+3)M+(4s+3r)C+3S$. In the particular case of a 2-isogeny the cost is $6M+3S+4C$. In the case of subgroups of order not divisible by 2 and 3 the cost is $(3r+3)M+3rC+3S$

5.4 Cost of Computing the Isogeny for Subgroup of Order 3 in Projective Coordinates

- First, second and third cases of Theorem 2. In these cases $g(x,y) = \big(m(XZ^2+X^2Y+Y^2Z) : m(YZ^2+Y^2X+X^2Z) : XYZ\big)$. The computation of X^2,Y^2,Z^2 and XYZ costs $3S+2M$. The computation of XY^2,X^2Y,XZ^2,Y^2Z,YZ^2 and X^2Z requires $6M$. Finally computing $m(XZ^2+X^2Y+Y^2Z)$ and $m(YZ^2+Y^2X+X^2Z)$ requires$2C$. For the second and third case of Theorem 2 we add $4C$ for computing jXZ^2,jYZ^2,j^2X^2Y and j^2Y^2X in the second case (resp jXZ^2,jYZ^2,j^2X^2Z and j^2Y^2Z in the third case). The total cost is $8M+3S+2C$ for the first case and $8M+3S+6C$ for the second and third case.
- Fourth case of Theorem 2. The isogeny is $g(x,y) = (m(-jX^3+Z^3-d(-1/3j+1/3)XYZ) : m(-jY^3+Z^3-d(-1/3j+1/3)XYZ) : XYZ)$. One computes X^3,Y^3, Z^3 and deduces $dXYZ = X^3+Y^3+Z^3$ and $XYZ = \frac{1}{d}(X^3+Y^3+Z^3)$at a cost of $3S+3M+C$. The computation of $-jX^3$, $-jY^3$ and $(-j/3+1/3)dXYZ$ requires $3C$. Finally the computation of $m(-jX^3+Z^3-d(-1/3j+1/3)XYZ)$ and $m(-jY^3+Z^3-d(-1/3j+1/3)XYZ)$ is done in $2C$. The total cost is $3M+3S+6C$

In the Table 1 we compare the cost of the Hessian isogeny obtained in this work with the cost of Edward, Huff and Jacobi quartic isogenies in the case of subgroup of order not divisible by 2 and 3. We can draw the conclusion that isogenies over Hessian curves are slightly efficient than the existing ones. In particular this work provides a fastest $(3M+3S+6C)$ degree-3 isogeny with respect to Edward $(6M+4S+3C)$, Huff $(7M+3S+4C)$ and Jacobi $(6M+3S+11C)$ isogenies.

6 Conclusion

In this paper we gave an analogue of Vélu's formulas on Hessian curves and the analysis of the cost of the computation of this map shows that Hessian isogenies are slightly faster than Edward isogenies, Jacobi and Huff isogenies. As isogenies have been used to improve the efficiency of many algorithms, it will be interesting to also implement these protocols with Hessian isogenies and to compare the efficiency.

References

1. Noam D. Alkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory, Proceedings*, pages 21–76, 1997.
2. Reza Azarderakhsh, Elena Bakos Lang, David Jao, and Brian Koziel. Edsidh: Supersingular isogeny diffie-hellman key exchange on edwards curves. In *Security, Privacy, and Applied Cryptography Engineering - 8th International Conference, SPACE 2018, Kanpur, India, December 15-19, 2018, Proceedings*, pages 125–141, 2018.
3. Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted Hessian Curves. In *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*, pages 269–294, 2015.
4. Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for CSIDH. In *Progress in Cryptology - LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2-4, 2019, Proceedings*, pages 173–193, 2019.
5. Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.
6. Joo Paulo da Silva, Ricardo Dahab, and Julio Lpez. 2-isogenies between elliptic curves in hesse model. In *Anais do XVIII Simpsio Brasileiro em Segurana da Informao e de Sistemas Computacionais*, pages 57–64. SBC, 2018.
7. Thinh Dang and Dustin Moody. Twisted hessian isogenies. *IACR Cryptology ePrint Archive*, 2019:1003, 2019.
8. Christophe Doche, Thomas Icart, and David R. Kohel. Efficient scalar multiplication by isogeny decompositions. In *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, pages 191–206, 2006.
9. Reza Rezaeian Farashahi and Marc Joye. Efficient arithmetic on hessian curves. In *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, pages 243–260, 2010.
10. Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Mathematical Cryptology*, 8(3):209–247, 2014.
11. Emmanuel Fouotsa. Parallelizing pairings on Hessian elliptic curves. *Arab Journal of Mathematical Sciences*, 25(1):29 – 42, 2019.
12. Mireille Fouquet and François Morain. Isogeny volcanoes and the SEA algorithm. In *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*, pages 276–291, 2002.
13. Steven D. Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. *J. Cryptology*, 24(3):446–469, 2011.
14. Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 190–200, 2001.
15. Haihua Gu, Dawu Gu, and WenLu Xie. Efficient pairing computation on elliptic curves in hessian form. In *Information Security and Cryptology - ICISC 2010 - 13th International Conference, Seoul, Korea, December 1-3, 2010, Revised Selected Papers*, pages 169–176, 2010.
16. Debiao He, Jianhua Chen, and Jin Hu. A random number generator based on isogenies operations. *IACR Cryptology ePrint Archive*, 2010:94, 2010.
17. T. Izu and T. Takagi. Exceptional procedure attack on elliptic curve cryptosystems. *PKC 2003 , LNCS, Springer*, vol. 2567, pp. 224-239, 2003.
18. Marc Joye and Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, number Generators, pages 402–410, 2001.
19. Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong, and Young-Ho Park. Efficient isogeny computations on twisted edwards curves. *Security and Communication Networks*, 2018:5747642:1–5747642:11, 2018.
20. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized method for computing odd-degree isogenies on edwards curves. *IACR Cryptology ePrint Archive*, 2019:110, 2019.
21. Perez Broon Fouazou Lontouo and Emmanuel Fouotsa. http://www.emmanuelfouotsa-prmais.org/Portals/22/HessianIsogenies.zip.

22. Michael Meyer and Steffen Reith. A faster way to the CSIDH. *IACR Cryptology ePrint Archive*, 2018:782, 2018.
23. Dustin Moody. Using 5-isogenies to quintuple points on elliptic curves. *Inf. Process. Lett.*, 111(7):314–317, 2011.
24. Dustin Moody and Daniel Shumow. Analogues of vélu's formulas for isogenies on alternate models of elliptic curves. *Math. Comput.*, 85(300):1929–1951, 2016.
25. Neriman Gamze Orhon and Hüseyin Hisil. Speeding up huff form of elliptic curves. *Des. Codes Cryptogr.*, 86(12):2807–2823, 2018.
26. Rene Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp*, 44(3):483–494, 1985.
27. Joao Paulo Da Silva and Julio Lopez annd Ricardo Dahab.
28. J.H. Silvermann. *The Arithmetic of elliptic curves*, volume 106 of graduate texts in Mathematics. Springer-Verlag, 2009.
29. Nigel P. Smart. The hessian form of an elliptic curve. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, number Generators, pages 118–125, 2001.
30. J. V'elu. Isogenies entre courbes elliptiques. 1971.
31. Xiu Xu, Wei Yu, Kunpeng Wang, and Xiaoyang He. Constructing isogenies on extended Jacobi quartic curves. In *Information Security and Cryptology - 12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers*, pages 416–427, 2016.