Research Article

Fouazou Lontouo Perez Broon, Thinh Dang, Emmanuel Fouotsa, and Dustin Moody*

Isogenies on twisted Hessian curves

https://doi.org/10.1515/jmc-2020-0037
Received Sep 10, 2020; accepted Jan 05, 2021

Abstract: Elliptic curves are typically defined by Weierstrass equations. Given a kernel, the well-known Vélu's formula shows how to explicitly write down an isogeny between Weierstrass curves. However, it is not clear how to do the same on other forms of elliptic curves without isomorphisms mapping to and from the Weierstrass form. Previous papers have shown some isogeny formulas for (twisted) Edwards, Huff, and Montgomery forms of elliptic curves. Continuing this line of work, this paper derives explicit formulas for isogenies between elliptic curves in (twisted) Hessian form. In addition, we examine the numbers of operations in the base field to compute the formulas. In comparison with other isogeny formulas, we note that our formulas for twisted Hessian curves have the lowest costs for processing the kernel and our X-affine formula has the lowest cost for processing an input point in affine coordinates.

Keywords: Elliptic curves, Isogeny, Hessian curves, Vélu's formulas

2020 Mathematics Subject Classification: 14H52; 14K02

1 Introduction

An elliptic curve is defined as a nonsingular irreducible projective curve of genus one, with a specified point as additive identity on the curve. An elliptic curve is said to be defined over a field k if the curve is defined over k and the specified point additive identity is k-rational.

Let E be an elliptic curve defined over k with the specified point additive identity O. It is well known that there exist functions $x, y \in k(E)$ such that the rational map ϕ defined over k by $\phi = (x : y : 1)$ is an isomorphism from E to an elliptic curve in Weierstrass form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and $\phi(O) = (0 : 1 : 0)$, where $a_1, a_2, \ldots, a_6 \in k$ (see [1, III.3.1]). Therefore, elliptic curves are typically identified with curves defined by such a Weierstrass equation with the specified point additive identity $(0 : 1 : 0)$.

Let E and E' be elliptic curves with specified point additive identities O and O' respectively. An isogeny from E to E' is defined as a morphism $\phi : E \to E'$ such that $\phi(O) = O'$. It is a theorem (see [1, III.4.8]) that an isogeny is also a group homomorphism. As a corollary, the kernel of an isogeny is a finite subgroup of the domain. Conversely, if F is a finite subgroup of E, there exists an elliptic curve E' and a separable isogeny

***Corresponding Author: Dustin Moody:** Computer Security Division, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD, 20899-8930, United States of America; Email: dustin.moody@nist.gov
Fouazou Lontouo Perez Broon: Department of Mathematics and Computer Sciences, Faculty of Sciences, The University of Maroua, P.O.Box 814 Maroua, Cameroon
Thinh Dang: Computer Security Division, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD, 20899-8930, United States of America; Department of Computer Science, George Washington University, United States of America
Emmanuel Fouotsa: Department of Mathematics, Higher Teacher Training College, The University of Bamenda, P.O BOX 39 Bambili, Cameroon
Emmanuel Fouotsa This author is supported by the PREMA project in Subsaharan Africa sponsoserd by The Simons Foundation

$\phi : E \to E'$ such that the kernel of ϕ is F (see [1, III.4.12]). Given E and F, Vélu's formula in [2] shows an explicit expression for ϕ and E', where E and E' are both in Weierstrass form.

However, the Weierstrass equation is only one way to represent an elliptic curve. Other forms of elliptic curves are possible and have been proposed, some with applications in cryptography. Examples include Montgomery curves in [3, 4], (twisted) Edwards curves in [5–7], Huff curves in [8, 9], and (twisted) Hessian curves in [10]. The first formulas for isogenies defined directly for non-Weierstrass curves was for (twisted) Edwards curves and Huff curves [11]. Shortly thereafter, similar work, [12] and [13], showed formulas for computing isogenies on Montgomery curves. In this paper, we derive a formula for isogenies on twisted Hessian curves and consider the computational cost of computing image points. Furthermore, in our main proof, we make explicit and rigorous the techniques and justifications that are required but omitted in proving isogeny formulas in previous works. Compared to other isogeny formulas, we note that our formulas for twisted Hessian curves have the lowest costs for preprocessing the kernel points to determine the rational map prior to input evaluation, and our X-affine formula has the lowest cost for processing an input point in affine coordinates.

Isogenies have found applications in counting the number of points on an elliptic curve over a finite field (e.g. see [14, 15]), analyzing the complexity of elliptic-curve discrete logarithms in [16], and cryptographic constructions (e.g. [17–19]). More efficient isogeny formulas could lead to performance benefits in the above applications.

The organization of the paper is as follows. Section 2 introduces Hessian curves and their generalization called twisted Hessian curves. A summary of the point addition formulas on twisted Hessian curves is included. Section 3 derives formulas for 3-isogenies. Section 4 states and proves the main result for isogenies with a kernel of size $\ell \not\equiv 0 \pmod 3$. Finally, Section 5 examines the main formula's computational cost of computing image points. Some open problems and directions for future work are given in Section 6.

2 Twisted Hessian Curves

A Hessian curve in projective coordinates is defined by the equation

$$X^3 + Y^3 + Z^3 = dXYZ$$

with $27 - d^3 \neq 0$. The Hessian form of elliptic curves has been studied, for example, in [20–23], to optimize point addition and scalar multiplication formulas, as well as to optimize pairing computations. In addition, as a step towards resistance against side-channel attacks, the Sylvester addition formula (described below) on Hessian curves can also be used for point doubling and subtraction after a permutation of input coordinates [24]. A generalization of Hessian curves, called twisted Hessian curves, is defined by the equation

$$aX^3 + Y^3 + Z^3 = dXYZ$$

with $a(27a - d^3) \neq 0$. Twisted Hessian curves were used in [10] to provide a complete unified addition formula and improve efficiency for point doubling and tripling over fields of arbitrary characteristic. Other works that optimized arithmetic on (twisted) Hessian curves include [25–27].

Definition 1. A *twisted Hessian curve* over a field k is a projective curve $H(a, d)$ defined by the polynomial $aX^3 + Y^3 + Z^3 = dXYZ$ with the specified point $(0 : -1 : 1)$ as additive identity in the projective space $\mathbb{P}(k)^2$, with $a, d \in k$ and $a(27a - d^3) \neq 0$. If $a = 1$, the curve is called a *Hessian curve*.

As an elliptic curve, each twisted Hessian curve must be isomorphic over k to a curve given by a Weierstrass equation. Over a finite field of characteristic not equal to 3, we can find an explicit isomorphism from any twisted Hessian curve to a Weierstrass curve, and conversely, from any Weierstrass curve with a k-rational point of order 3 to a twisted Hessian curve. Such isomorphisms are given in [10, Theorem 5.3 and 5.4] and [28].

For convenience, we summarize below the formulas for point addition on twisted Hessian curves. Let $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ be points on $H(a, d)$. The inverse of $(X_1 : Y_1 : Z_1)$ is

$$-(X_1 : Y_1 : Z_1) = (X_1 : Z_1 : Y_1).$$

The (Sylvester) standard addition formula is given by:

$$\begin{aligned} X_3 &= X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1, \\ Y_3 &= Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1, \\ Z_3 &= Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1. \end{aligned}$$

If $(X_3, Y_3, Z_3) \neq (0, 0, 0)$, then $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$. Another addition formula, called *rotated addition*, is defined by the formula:

$$\begin{aligned} X_3' &= Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2, \\ Y_3' &= Y_2^2 Y_1 Z_1 - a X_1^2 X_2 Z_2, \\ Z_3' &= a X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2. \end{aligned}$$

If $(X_3', Y_3', Z_3') \neq (0, 0, 0)$, then $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3' : Y_3' : Z_3')$. The completeness follows because $(X_3, Y_3, Z_3) \neq (0, 0, 0)$ or $(X_3', Y_3', Z_3') \neq (0, 0, 0)$ by [10, Theorem 4.7]. Moreover, if a is not a cube in k, then $(X_3', Y_3', Z_3') \neq (0, 0, 0)$ [10, Theorem 4.5].

3 3-isogenies

In this section, we show how to compute 3-isogenies on twisted Hessian curves, and in the next section, we provide a formula for ℓ-isogenies with $\ell \not\equiv 0 \pmod 3$. To compute an isogeny with kernel of size divisible by 3, we can write the kernel as an internal product of a subgroup of size ℓ not divisible by 3 and one or more subgroups of size 3, and compose the formulas for each factor. Together, these formulas are sufficient for kernels of any size. In particular, to obtain an isogeny with kernel of size $3^r \ell$ where $\ell \not\equiv 0 \pmod 3$, we can compose an ℓ-isogeny with r isogenies of degree 3.

To derive the result for 3-isogenies, we begin by characterizing all points of order 3 on a twisted Hessian curve. Let c be a cubic root of a. It can be easily verified that the point $(1 : 0 : -c)$ and its inverse $(1 : -c : 0)$ both have order 3. In addition, if $\omega^3 = 1$ and $\omega \neq 1$, then $(0 : -\omega : 1)$ and its inverse $(0 : 1 : -\omega)$ have order 3. The verification has been done in [10, Theorem 5.1]. In fact, based on the cardinality of the 3-torsion on elliptic curves (e.g. see [29, Theorem 3.2]), these are the only points of order 3 on a twisted Hessian curve. Moreover, using the defining equation of $H(a, d)$, it can be easily verified that the 3-torsion is the precisely the set of points $(X : Y : Z)$ such that $XYZ = 0$.

We now turn to formulas for 3-isogenies of twisted Hessian curves. As seen in the preceding paragraph, a kernel of size 3 is either generated by $(0 : -\omega : 1)$ with $\omega^3 = 1$ and $\omega \neq 1$ or by $(1 : -c : 0)$ with $c^3 = a$. First, we consider 3-isogenies with their kernel generated by $(0 : -\omega : 1)$. Such a map can be obtained by composing the 3-isogeny given in [10, Theorem 5.4] from a twisted Hessian curve to a Weierstrass curve of the form $Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3$ with the isomorphism given in [10, Theorem 5.4] between such a Weierstrass curve and a twisted Hessian curve. The result of such composition is stated in Theorem 1.

Theorem 1. *Let $\omega^3 = 1$ and $\omega \neq 1$. The map*

$$(X : Y : Z) \mapsto (XYZ : aX^3 + \omega^2 Y^3 + \omega Z^3 : aX^3 + \omega Y^3 + \omega^2 Z^3)$$

is an isogeny from $H(a, d)$ to $H(d^3 - 27a, 3d)$ with the kernel

$$\langle (0 : -\omega : 1) \rangle = \langle (0 : -\omega^2 : 1) \rangle = \{(0 : -1 : 1), (0 : -\omega : 1), (0 : -\omega^2 : 1)\}.$$

Proof. We leave the straightforward verification to the reader. □

Next, we consider 3-isogenies with kernel generated by the point $(1 : -c : 0)$ with $c^3 = a$. The only formula for such isogenies that we are aware of is given in [30, Proposition 4] for Hessian curves over characteristic 3. We restate the result here.

Theorem 2. *Let k have characteristic 3. The map $\sigma : H(1, d^{3^{i+1}}) \to H(1, d^{3^i})$ defined by*

$$\sigma(X : Y : Z) = (d^{2\cdot 3^i} XYZ : Y^2Z + X^2Y + XZ^2 : XY^2 + X^2Z + YZ^2)$$

is an isogeny. Moreover, $f : H(1, d^{3^i}) \to H(1, d^{3^{i+1}})$ defined by $f(X : Y : Z) = (X^3 : Y^3 : Z^3)$ is an isogeny, and $f \circ \sigma(P) = 3P$ for each P on $H(1, d^{3^{i+1}})$. The kernel of σ is $\{(0 : -1 : 1), (-1 : 1 : 0), (-1 : 0 : 1)\}$.

We generalize Theorem 2 to 3-isogenies on twisted Hessian curves $H(a, d)$ over any characteristic with kernel $\langle(1 : -c : 0)\rangle$, where $c^3 = a$.

Theorem 3. *The rational map*

$$\phi = \left(XYZ : c^2X^2Z + cXY^2 + YZ^2 : c^2X^2Y + cXZ^2 + Y^2Z\right).$$

is an isogeny from $H(a, d)$ to $H(A, D)$, where $c^3 = a$,

$$A = d^2c + 3dc^2 + 9a \text{ and } D = d + 6c$$

with kernel

$$\langle(1 : -c : 0)\rangle = \langle(1 : 0 : -c)\rangle = \{(0 : -1 : 1), (1 : -c : 0), (1 : 0 : -c)\}.$$

Proof. Let $f = xy$, $g = c^2x^2 + cxy^2 + y$, and $h = c^2x^2y + cx + y^2$ be the dehomogenized coordinate maps of ϕ. Also let A and D be as given in the theorem statement. Then,

$$Af^3 + g^3 + h^3 - Dfgh = (ax^3y^3 - cdx^2y^2 + ax^3 + y^3)(ax^3 + y^3 + 1 - dxy).$$

This shows that the range of the rational map ϕ is indeed $H(A, D)$. It remains to check that the kernel is as claimed. Let $P = (X : Y : Z)$ and suppose $\phi(P) = (0 : -1 : 1)$, then $XYZ = 0$.

1. If $X = 0$, then $YZ^2 = -Y^2Z$, i.e. $Z = -Y$ and $P = (0 : -1 : 1)$.
2. If $Y = 0$, then $c^2X^2Z = -cXZ^2$, i.e. $cX = -Z$ and $P = (1 : 0 : -c)$.
3. If $Z = 0$, then $cXY^2 = -c^2X^2Y$, i.e. $Y = -cX$ and $P = (1 : -c : 0)$.

Conversely, by straightforward calculation, we see that $\phi(P) = (0 : -1 : 1)$ for each such P. □

4 Isogenies of degree $\ell \not\equiv 0 \pmod 3$

In this section, we look at the ℓ-isogeny formulas, where $\ell \not\equiv 0 \pmod 3$. One approach for obtaining such an ℓ-isogeny between twisted Hessian curves is to compose the isogeny given by Vélu's formula with isomorphisms to and from Weierstrass curves. This approach, however, doesn't lead to a simple formula. Moreover, the resulting codomain twisted Hessian curve is dependent on the choice of point of order 3 on the codomain Weierstrass curve produced by Vélu's formula. We prove our main twisted Hessian isogeny result as follows.

Theorem 4. *Let $F = \{(0 : -1 : 1)\} \cup \{(s_i : t_i : 1)\}_{i=1}^n$ be a finite subgroup of $H(a, d)$ of size $\ell = n + 1$, where ℓ is not divisible by 3. Then, F is the kernel of an isogeny from $H(a, d)$ to $H(A, D)$ defined by*

$$\phi(P) = \left(\prod_{R\in F} X(P + R) : \prod_{R\in F} Y(P + R) : \prod_{R\in F} Z(P + R)\right).$$

where $A = a^\ell$ *and*

$$D = \frac{(1-2n)d + 6\sum_{i=1}^{n} 1/(s_i t_i)}{\prod_{i=1}^{n} s_i}.$$

Note that in the equation for ϕ, for each point $P + R$, the choice of representative of $P + R$ in projective coordinates does not affect the result $\phi(P)$. Moreover, $s_i t_i \neq 0$ for each $i \in \{1, 2, \ldots, n\}$.

Proof. Without loss of generality, let k be algebraically closed. We start by writing down a rational form of the map ϕ given in the theorem, which is derived from the standard addition formula. Let

$$\phi_Y := \frac{y}{x}\prod_{i=1}^{n}\frac{xy - s_i t_i}{s_i^2 y - t_i x^2} \text{ and } \phi_Z := \frac{1}{x}\prod_{i=1}^{n}\frac{t_i^2 x - s_i y^2}{s_i^2 y - t_i x^2}.$$

That is, $\phi(x : y : 1) = (1 : \phi_Y : \phi_Z)$. Define

$$G = A + \phi_Y^3 + \phi_Z^3 - D\phi_Y\phi_Z \in k(H),$$

where $A, D \in k$ are to be determined.

Our goal is show that $G = 0$ for $A, D \in k$ as stated in the theorem. To this end, by Proposition [1, II.1.2], it suffices to show that G has no poles and $G(Q) = 0$ for some Q on H. By the definitions of ϕ_Y and ϕ_Z, if P is a pole of G, then $X(\phi(P)) = 0$, which is equivalent to $X(P+R) = 0$ for some $R \in F$. Let $Q = P+R$. From the formula of ϕ, it can be seen that ϕ is invariant under translation by any point in F. So $\phi(P) = \phi(Q)$ and $X(Q) = 0$. Therefore, if G has a pole at some point P, then G also has a pole at some point Q with $X(Q) = 0$. By subsituting $X = 0$ into the defining equation of H, we find that the only points Q with $X(Q) = 0$ are $\{(0 : -\omega : 1) \mid \omega^3 = 1\}$.

Let $P = (0 : -\omega : 1)$ with $\omega^3 = 1$. We'll show that P is not a pole of G for some A and D in k and hence by the arguments in the preceding paragraph, G has no pole at all and thus is constant.

First, we assume that the characteristic of k is not 3. We need the following facts:

- $k[H]_P$ is a discrete valuation ring and x is a uniformizer of $k[H]_P$ by [31, Theorem 1 of Chapter 3].
- $k[H]_P$ has the unique maximal ideal $M_P := \{q \in k[H]_P \mid q(P) = 0\}$ (see [31, Section 2.4]).
- $k(H)$ is the field of quotients of $k[H]_P$.
- The field k is a subring of $k[H]_P$, and the map $b \mapsto b + M_p$ from k to $k[H]_p/M_P$ is a field isomorphism.

We can conclude that the function that maps each element in $k(H)$ to its Laurent series expansion in $k((x))$ is a one-to-one ring homomorphism [31, Problem 2.32]. We write $f = \sum_{i=m}^{r} c_i x^i$ where $m \in \mathbb{Z}$ and $r \in \mathbb{Z} \cup \{\infty\}$ to mean that f has the Laurent series expansion $\sum_{i=m}^{r} c_i x^i$. We also denote by $O(x^n)$ any unspecified series of order at least n.

Next, we find the series expansion of y in terms of x. The order of y at P is $\mathrm{ord}_P(y) = 0$, since y is defined and is nonzero at P. Thus y has a power series expansion $y = \sum_{i=0}^{\infty} c_i x^i$. As $ax^3 + y^3 + 1 - dxy$ is zero in $k(H)$ and the function that maps each element in $k(H)$ to its Laurent series expansion is a one-to-one ring homomorphism,

$$ax^3 + (\sum_{i=0}^{\infty} c_i x^i)^3 + 1 - dx(\sum_{i=0}^{\infty} c_i x^i) = 0.$$

Since $y - c_0$ vanishes at P, we have $c_0 = -\omega$. Then, solving for c_1 and c_2 gives

$$y = -\omega - \frac{d}{3\omega}x + O(x^3).$$

Then,

$$\frac{xy - s_i t_i}{s_i^2 y - t_i x^2} = \frac{t_i}{\omega s_i} + \left(\frac{3 - d s_i t_i}{3 s_i^2}\right)x + \left(\frac{9t_i^2 - d^2 s_i^2 t_i}{9\omega^2 s_i^3}\right)x^2 + O(x^3),$$

$$\frac{t_i^2 x - s_i y^2}{s_i^2 y - t_i x^2} = \frac{\omega}{s_i} + \left(\frac{3t^2 - ds}{3\omega s^2}\right)x + \left(\frac{d s_i t_i^2 - 3t}{3 s_i^3}\right)x^2 + O(x^3).$$

Note that by the characterization of the 3-torsion in the preceding section, that the kernel does not contain a point of order 3 is equivalent to $s_i t_i \neq 0$. In the remainder of the proof, we use the definition $S := \prod_{i=1}^{n} s_i$, and since $-(s_i : t_i : 1) = (s_i/t_i : 1/t_i : 1)$, we have

$$\prod_{i=1}^{n} t_i = 1, \quad \sum_{i=1}^{n} \frac{t_i^2}{s_i} = \sum_{i=1}^{n} \frac{1}{s_i t_i}, \quad \text{and} \quad \sum_{1\le i<j\le n} \frac{t_i^2 t_j^2}{s_i s_j} = \sum_{1\le i<j\le n} \frac{1}{s_i s_j t_i t_j}. \tag{1}$$

Moreover, we also use the following formula for the product of power series:

$$\begin{aligned}
&\prod_{i=1}^{n} c_i^{(0)} + c_i^{(1)} x + c_i^{(2)} x^2 + O(x^3) \\
&\qquad = \prod_{i=1}^{n} c_i^{(0)} + \Big(\prod_{i=1}^{n} c_i^{(0)}\Big)\Big(\sum_{i=1}^{n} \frac{c_i^{(1)}}{c_i^{(0)}}\Big) x \\
&\qquad\qquad + \Big(\prod_{i=1}^{n} c_i^{(0)}\Big)\Big(\sum_{i=1}^{n} \frac{c_i^{(2)}}{c_i^{(0)}} + \sum_{1\le i<j\le n} \frac{c_i^{(1)} c_j^{(1)}}{c_i^{(0)} c_j^{(0)}}\Big) x^2 + O(x^3),
\end{aligned}$$

assuming $\prod_{i=1}^{n} c_i^{(0)} \neq 0$.

Thus, we have

$$\prod_{i=1}^{n} \frac{xy - s_i t_i}{s_i^2 y - t_i x^2} = U_0 + U_1 x + U_2 x^2 + O(x^3),$$

where

$$\begin{aligned}
U_0 &= \prod_{i=1}^{n} \frac{t_i}{\omega s_i} = \frac{1}{\omega^n S}, \\
U_1 &= \Big(\prod_{i=1}^{n} \frac{t_i}{\omega s_i}\Big) \sum_{i=1}^{n} \Big(\frac{\omega}{s_i t_i} - \frac{d}{3}\Big) = \frac{1}{\omega^{n-1} S}\Big(-\frac{nd}{3} + \sum_{i=1}^{n} \frac{1}{s_i t_i}\Big), \\
U_2 &= \prod_{i=1}^{n} \frac{t_i}{\omega s_i}\Big(\sum_{i=1}^{n} \Big(\frac{d^2}{9\omega} - \frac{t_i}{\omega s_i^2}\Big) + \sum_{1\le i<j\le n} \Big(\frac{\omega^2 (3 - d s_i t_i)(3 - d s_j t_j)}{9 s_i s_j t_i t_j}\Big)\Big) \\
&= \frac{1}{\omega^n S}\Big(\sum_{i=1}^{n} \Big(\frac{d^2}{9\omega} - \frac{t_i}{\omega s_i^2}\Big) + \sum_{1\le i<j\le n} \Big(\frac{d^2\omega^2}{9} - \frac{d\omega^2}{3 s_i t_i} - \frac{d\omega^2}{3 s_j t_j} + \frac{\omega^2}{s_i s_j t_i t_j}\Big)\Big) \\
&= \frac{1}{\omega^{n+1} S}\Big(\frac{n(n+1)}{2}\frac{d^2}{9} - \sum_{i=1}^{n} \frac{t_i}{s_i^2} - \frac{(n-1)d}{3}\sum_{i} \frac{1}{s_i t_i} + \sum_{1\le i<j\le n} \frac{1}{s_i s_j t_i t_j}\Big).
\end{aligned}$$

Moreover,

$$\prod_{i=1}^{n} \frac{t_i^2 x - s_i y^2}{s_i^2 y - t_i x^2} = V_0 + V_1 x + V_2 x^2 + O(x^3),$$

where

$$\begin{aligned}
V_0 &= \prod_{i=1}^{n} \frac{\omega}{s_i} = \frac{\omega^n}{S}, \\
V_1 &= \frac{\omega^n}{S} \sum_{i=1}^{n} \frac{d}{3\omega^2} - \frac{t_i^2}{\omega^2 s_i} = \frac{\omega^{n-2}}{S}\Big(\frac{nd}{3} - \sum_{i=1}^{n} \frac{t_i^2}{s_i}\Big), \\
V_2 &= \frac{\omega^n}{S}\Big(\sum_{i=1}^{n} \Big(\frac{d t_i^2}{3\omega s_i} - \frac{t_i}{\omega s_i^2}\Big) + \sum_{1\le i<j\le n} \frac{(d s_i - 3t_i^2)(d s_j - 3t_j^2)}{9\omega^4 s_i s_j}\Big)
\end{aligned}$$

$$= \frac{\omega^n}{S}\Big(\sum_{i=1}^{n}\big(\frac{dt_i^2}{3\omega s_i} - \frac{t_i}{\omega s_i^2}\big) + \sum_{1\le i<j\le n}\frac{d^2}{9\omega} - \frac{dt_i^2}{3\omega s_i} - \frac{dt_j^2}{3\omega s_j} + \frac{t_i^2 t_j^2}{\omega s_i s_j}\Big)$$
$$= \frac{\omega^{n-1}}{S}\Big(\frac{n(n-1)}{2}\frac{d^2}{9} - \sum_{i=1}^{n}\frac{t_i}{s_i^2} + \frac{(2-n)d}{3}\sum_{i=1}^{n}\frac{t_i^2}{s_i} + \sum_{1\le i<j\le n}\frac{t_i^2 t_j^2}{s_i s_j}\Big).$$

Substitution into G, with some additional simplifying using (1), yields

$$G = G_{-3}x^{-3} + G_{-2}x^{-2} + G_{-1}x^{-1} + O(1),$$

where

$$G_{-3} = 0,$$
$$G_{-2} = \frac{\omega}{S^3}\Big((2n-1)d - 6\sum_{i=1}^{n}\frac{1}{s_i t_i} + DS\Big),$$
$$G_{-1} = \frac{\omega^2 d}{3S^3}\Big((2n-1)d - 6\sum_{i=1}^{n}\frac{1}{s_i t_i} + DS\Big).$$

Hence, $G_{-2} = G_{-1} = 0$ if

$$D = \frac{(1-2n)d + 6\sum_{i=1}^{n}\frac{1}{s_i t_i}}{S};$$

i.e. G has no pole and thus is constant.

Finally, we consider the case when k has characteristic 3. In particular, x is not a uniformizer for $k[H]_P$. Instead, $\omega = 1$, and $u = y + 1$ is a uniformizer for $k[H]_P$. Since x is defined and vanishes at P, i.e. $\mathrm{ord}_P(x) \ge 1$, x has a power series expansion $x = \sum_{i=0}^{\infty} b_i u^i$ with $b_0 = 0$. Hence,

$$a(\sum_{i=0}^{\infty} b_i u^i)^3 + (u-1)^3 + 1 - d(\sum_{i=0}^{\infty} b_i u^i)(u-1) = 0.$$

Solving for $b_1, b_2, \ldots$, we get

$$x = -\frac{1}{d}(u^3 + u^4 + \cdots + u^8) + \frac{a-d^3}{d^4}(u^9 + \cdots + u^{11}) + \frac{-a-d^3}{d^4}(u^{12} + u^{13} + u^{14}) + O(u^{15}).$$

Note that in characteristic 3, by the definition of twisted Hessian curves, $d \neq 0$. Then,

$$(\frac{xy - s_i t_i}{s_i^2 y - t_i x^2})^3 = \frac{t_i^3}{s_i^3}(1 + u^3 + u^6) + O(u^9),$$
$$(\frac{t_i^2 x - s_i y^2}{s_i^2 y - t_i x^2})^3 = \frac{1}{s_i^3}(1 - u^3) + O(u^9),$$
$$\frac{xy - s_i t_i}{s_i^2 y - t_i x^2}\cdot\frac{t_i^2 x - s_i y^2}{s_i^2 y - t_i x^2} = \frac{1}{s_i^2}\Big(t_i + \frac{t_i^3 + 2}{d s_i}u^3 + \frac{t_i^3}{d s_i}u^6\Big) + O(u^9).$$

Therefore,

$$\prod_{i=1}^{n}(\frac{xy - s_i t_i}{s_i^2 y - t_i x^2})^3 = \frac{1}{S^3}\Big(1 + nu^3 + \frac{n(n+1)}{2}u^6\Big) + O(u^9),$$
$$\prod_{i=1}^{n}(\frac{t_i^2 x - s_i y^2}{s_i^2 y - t_i x^2})^3 = \frac{1}{S^3}\Big(1 - nu^3 + \frac{n(n-1)}{2}u^6\Big) + O(u^9),$$
$$\prod_{i=1}^{n}\frac{xy - s_i t_i}{s_i^2 y - t_i x^2}\cdot\frac{t_i^2 x - s_i y^2}{s_i^2 y - t_i x^2} = \frac{1}{S^2}\Big(1 + \sum_{i=1}^{n}\frac{t_i^3 + 2}{d s_i t_i}u^3\Big) + O(u^6).$$

Using the identities in (1), since

$$\sum_{i=1}^{n} \frac{(t_i^3+2)}{ds_it_i} = \frac{1}{d}\Big(\sum_{i=1}^{n} \frac{t_i^2}{s_i} - \sum_{i=1}^{n} \frac{1}{s_it_i}\Big) = 0,$$

we obtain the simplified expression

$$\prod_{i=1}^{n} \frac{xy - s_it_i}{s_i^2y - t_ix^2} \cdot \frac{t_i^2x - s_iy^2}{s_i^2y - t_ix^2} = \frac{1}{S^2} + O(u^6).$$

Substitution into the definition of G, with additional simplification in characteristic 3, yields

$$G = \frac{d^2DS + (2n-1)d^3}{S^3}u^{-6} + \frac{-d^2DS + (1-2n)d^3}{S^3}u^{-3} + O(1).$$

Therefore, if $D = (1-2n)d/S$, $G = O(1)$ and thus is constant.

We have proved that for the value of D stated in theorem, G is constant. So if $G(Q) = 0$ for some Q, then $G = 0$. Next, we find $A \in k$ such that G vanishes at $Q = (1 : -c : 0) \in H$ where $c^3 = a$. By [10, Theorem 4.1], i.e. $(X : Y : Z) + (1 : -c : 0) = (Y : cZ : c^2X)$,

$$\begin{aligned}
\phi(Q) &= \left(\prod_{R\in F} X(Q+R) : \prod_{R\in F} Y(Q+R) : \prod_{R\in F} Z(Q+R)\right) \\
&= \left(\prod_{R\in F} Y(R) : c^\ell \prod_{R\in F} Z(R) : c^{2\ell} \prod_{R\in F} X(R)\right) \\
&= \left(\prod_{R\in F} Y(R)/Z(R) : c^\ell : 0\right) \\
&= (-1 : c^\ell : 0).
\end{aligned}$$

So $G(Q) = A - c^{3\ell} = A - a^\ell$. Solving $G(Q) = 0$ for A gives $A = a^\ell$.

It remains to check that the kernel of ϕ is indeed F. It's clear that $\phi(P) = (0 : -1 : 1)$ if $P \in F$. For the converse, suppose $\phi(P) = (0 : -1 : 1)$. Then $X(Q) = 0$ where $Q = P + R$ for some $R \in F$. So $Q = (0 : -1 : 1)$ or $Q = (0 : -\omega : 1)$ for some $\omega \neq 1$ such that $\omega^3 = 1$. If $Q = (0 : -1 : 1)$, $P = -R \in F$. Else, by [10, Theorem 4.6],

$$\phi(Q) = \phi(0 : -\omega : 1) = (0 : -\omega^\ell : 1) \neq (0 : -1 : 1)$$

since $3 \nmid \ell$. However, this contradicts $\phi(Q) = \phi(P) = (0 : -1 : 1)$. That concludes the proof.

□

5 Rational-map representations

In this section, we derive efficient rational-map representations of the isogeny in Theorem 4 and examine their computational complexity by counting the number of multiplications, squarings, and inversions. We denote by S, M, M_a, and I the cost of squaring, multiplication, multiplication by a, and inversion respectively.

In general, the computational cost depends on many factors, for examples, how the points are represented: projective, affine, or both (mixed), how much we want to avoid inversions, how the coordinate maps are represented (e.g. polynomials or rational functions), and the particular applications and their amortized running time. In our analysis, we will work with purely affine coordinates or purely projective coordinates, and allow up to one inversion operation. Furthermore, we separate the computation into two parts: one that involves only the kernel and one that requires the input point.

5.1 Affine coordinates

Due to the symmetry between the Z and Y coordinates, we have a choice whether to work with the X-affine and Z-affine patch. We will analyze both cases.

5.1.1 Z-affine coordinates

Lemma 1. *If $ax^3 + y^3 + 1 = dxy$ and $a\alpha^3 + \beta^3 + 1 = d\alpha\beta$, then,*

$$(xy - \alpha\beta)(\beta^2 xy - \alpha) = (\beta y^2 - a\alpha^2 x)(\beta x^2 - \alpha^2 y), \tag{2}$$
$$(\beta^2 y - a\alpha x^2)(y - a\alpha\beta x^2) = (\beta y^2 - a\alpha^2 x)(\beta - a\alpha^2 xy), \tag{3}$$
$$(\alpha y^2 - \beta^2 x)(\alpha\beta y^2 - x) = (\alpha^2 y - \beta x^2)(a\alpha^2 xy - \beta). \tag{4}$$

Proof. The lemma is implied by the following polynomial identities:

$$(xy - \alpha\beta)(\beta^2 xy - \alpha) - (\beta y^2 - a\alpha^2 x)(\beta x^2 - \alpha^2 y) = \alpha^2\beta(ax^3 + y^3 + 1 - dxy) - \alpha xy(a\alpha^3 + \beta^3 + 1 - d\alpha\beta),$$

$$(\beta^2 y - a\alpha x^2)(y - a\alpha\beta x^2) - (\beta y^2 - a\alpha^2 x)(\beta - a\alpha^2 xy) = a\alpha^2\beta x(ax^3 + y^3 + 1 - dxy) - a\alpha x^2 y(a\alpha^3 + \beta^3 + 1 - d\alpha\beta),$$

$$(\alpha y^2 - \beta^2 x)(\alpha\beta y^2 - x) - (\alpha^2 y - \beta x^2)(a\alpha^2 xy - \beta) = \alpha^2\beta y(ax^3 + y^3 + 1 - dxy) - \alpha xy^2(a\alpha^3 + \beta^3 + 1 - d\alpha\beta).$$

□

Corollary 1. *Let $F = \{(0, -1)\} \cup \{(\tilde{\alpha}_i, 1)\}_{i=1}^r \cup \{(\alpha_i, \beta_i), (\alpha_i/\beta_i, 1/\beta_i)\}_{i=1}^s$ be a subgroup of $H(a, d)$ and $|F| \not\equiv 0 \pmod 3$, where (α_i, β_i) has order greater than 2 and $(\tilde{\alpha}_i, 1)$ has order 2. Let ϕ be the isogeny in Theorem 4 with kernel F. Then,*

$$\phi = \left(x\prod_{i=1}^r \frac{\tilde{\alpha}_i - xy}{a\tilde{\alpha}_i x^2 - y}\prod_{i=1}^s \frac{\beta_i x^2 - \alpha_i^2 y}{\beta_i - a\alpha_i^2 xy}, y\prod_{i=1}^r \frac{y^2 - a\tilde{\alpha}_i^2 x}{a\tilde{\alpha}_i x^2 - y}\prod_{i=1}^s \frac{\beta_i y^2 - a\alpha_i^2 x}{\beta_i - a\alpha_i^2 xy}\right) \tag{5}$$
$$= \left(x\prod_{i=1}^r \frac{\tilde{\alpha}_i^2 y - x^2}{x - \tilde{\alpha}_i y^2}\prod_{i=1}^s \frac{\alpha_i^2 y - \beta_i x^2}{a\alpha_i^2 xy - \beta_i}, y\prod_{i=1}^r \frac{xy - \tilde{\alpha}_i}{x - \tilde{\alpha}_i y^2}\prod_{i=1}^s \frac{a\alpha_i^2 x - \beta_i y^2}{a\alpha_i^2 xy - \beta_i}\right). \tag{6}$$

Proof. Equation (5) follows from Theorem 4, the rotated addition formula, and simplification using equations (2) and (3) in Lemma 1. Equation (6) follows from Theorem 4, the standard addition formula, and simplification using equations (2) and (4) in Lemma 1. □

In counting the number of operations, we separate the computation into two parts: one that involves only the kernel and one that requires the input point. First, we look at (5).

- To process the kernel, we compute the following values: $\{\alpha_i^2, a\alpha_i, a\alpha_i^2\}_{i=1}^s$ and $\{a\tilde{\alpha}_i, a\tilde{\alpha}_i^2\}_{i=1}^r$. This step takes $sS + (2s + r)M_a + rM$.
- Then, we compute xy, x^2, y^2 for $2S + 1M$.
- Next, we compute $\{\beta_i x^2 - \alpha_i^2 y, \beta_i y^2 - a\alpha_i^2 x, \beta_i - a\alpha_i^2 xy\}_{i=1}^s$ and $\{y^2 - a\tilde{\alpha}_i^2 x, a\tilde{\alpha}_i x^2 - y\}_{i=1}^r$ for $(5s + 2r)M$
- The products $x(\prod_{i=1}^r \tilde{\alpha}_i - xy)(\prod_{i=1}^s \beta_i x^2 - \alpha_i^2 y)$, $y(\prod_{i=1}^r y^2 - a\tilde{\alpha}_i^2 x)(\prod_{i=1}^s \beta_i y^2 - a\alpha_i^2 x)$, and $(\prod_{i=1}^r a\tilde{\alpha}_i x^2 - y)(\prod_{i=1}^s \beta_i - a\alpha_i^2 xy)$ take additional $(3r + 3s - 1)M$.
- A final step takes $2M + 1I$.

In total, processing the kernel takes $sS + (2s + r)M_a + rM$ and the input point takes $2S + (8s + 5r + 2)M + 1I$. By similar counting, using (6), processing the kernel takes $(r + s)S + 2sM_a$ and the input point takes $2S + (8s + 5r + 2)M + 1I$.

5.1.2 X-affine coordinates

Lemma 2. *If $a + y^3 + z^3 = dyz$ and $a + \beta^3 + \gamma^3 = d\beta\gamma$, then,*

$$(\gamma^2 yz - a\beta)(\beta^2 yz - a\gamma) = (az - \beta\gamma y^2)(ay - \beta\gamma z^2), \tag{7}$$

$$(\gamma^2 y - \beta z^2)(\beta^2 y - \gamma z^2) = (az - \beta\gamma y^2)(yz - \beta\gamma), \tag{8}$$
$$(\beta^2 z - \gamma y^2)(\gamma^2 z - \beta y^2) = (yz - \beta\gamma)(ay - \beta\gamma z^2). \tag{9}$$

Proof.

$$(\gamma^2 yz - a\beta)(\beta^2 yz - a\gamma) - (ax - \beta\gamma y^2)(ay - \beta\gamma z^2) = a\beta\gamma(a + y^3 + z^3 - dyz) - ayz(a + \beta^3 + \gamma^3 - d\beta\gamma),$$

$$(\gamma^2 y - \beta z^2)(\beta^2 y - \gamma z^2) - (ax - \beta\gamma y^2)(yz - \beta\gamma) = \beta\gamma z(a + y^3 + z^3 - dyz) - yz^2(a + \beta^3 + \gamma^3 - d\beta\gamma),$$

$$(\beta^2 z - \gamma y^2)(\gamma^2 z - \beta y^2) - (yz - \beta\gamma)(ay - \beta\gamma z^2) = \beta\gamma y(a + y^3 + z^3 - dyz) - y^2 z(a + \beta^3 + \gamma^3 - d\beta\gamma).$$

□

Corollary 2. *Let* $F = \mathcal{O} \cup \{(\tilde{\beta}_i, \tilde{\beta}_i)\}_{i=1}^{r} \cup \{(\beta_i, \gamma_i), (\gamma_i, \beta_i)\}_{i=1}^{s}$ *be a subgroup of* $H(a, d)$ *and* $|F| \not\equiv 0 \pmod 3$*, where* (β_i, γ_i) *has order greater than 2 and* $(\tilde{\beta}_i, \tilde{\beta}_i)$ *has order 2. Let* ϕ *be the isogeny in Theorem 4 with kernel* F*. Then,*

$$\phi = \left(y \prod_{i=1}^{r} \frac{\tilde{\beta}_i^2 y^2 - az}{\tilde{\beta}_i(z^2 - \tilde{\beta}_i y)} \prod_{i=1}^{s} \frac{az - \beta_i\gamma_i y^2}{yz - \beta_i\gamma_i}, z \prod_{i=1}^{r} \frac{a - \tilde{\beta}_i yz}{z^2 - \tilde{\beta}_i y} \prod_{i=1}^{s} \frac{ay - \beta_i\gamma_i z^2}{yz - \beta_i\gamma_i}\right) \tag{10}$$
$$= \left(y \prod_{i=1}^{r} \frac{\tilde{\beta}_i^2 y - \tilde{\beta}_i z^2}{yz - \tilde{\beta}_i^2} \prod_{i=1}^{s} \frac{az - \beta_i\gamma_i y^2}{yz - \beta_i\gamma_i}, z \prod_{i=1}^{r} \frac{\tilde{\beta}_i^2 z - \tilde{\beta}_i y^2}{yz - \tilde{\beta}_i^2} \prod_{i=1}^{s} \frac{ay - \beta_i\gamma_i z^2}{yz - \beta_i\gamma_i}\right). \tag{11}$$

Moreover, using the notation of Theorem 4,

$$D = \prod_{i=1}^{r} \tilde{\beta}_i \left(\prod_{i=1}^{s} \beta_i\gamma_i \left((1 - 2r + 2s)d + 6 \sum_{i=1}^{r} \tilde{\beta}_i \right) - 6a \sum_{i=1}^{s} \prod_{j \neq i} \beta_j\gamma_j \right).$$

Note that the expression for D doesn't involve any inversion.

Proof. Equation (10) follows from Theorem 4, the rotated addition formula, and simplification using equations (7) and (8) in Lemma 2. Equation (11) follows from Theorem 4, the standard addition formula, and simplification using equations (8) and (9) in Lemma 2. The expression for D follows because, using the notation in Theorem 4,

$$\begin{aligned} \prod_{i=1}^{n} \frac{1}{s_i t_i} &= \sum_{i=1}^{s} \frac{\beta_i^3 + \gamma_i^3}{\beta_i\gamma_i} + \sum_{i=1}^{r} \tilde{\beta}_i = \sum_{i=1}^{s} \frac{d\beta_i\gamma_i - a}{\beta_i\gamma_i} + \sum_{i=1}^{r} \tilde{\beta}_i \\ &= sd - a \sum_{i=1}^{s} \frac{1}{\beta_i\gamma_i} + \sum_{i=1}^{r} \tilde{\beta}_i, \\ 1/\prod_{i=1}^{n} s_i &= \prod_{i=1}^{s} \beta_i\gamma_i \prod_{i=1}^{r} \tilde{\beta}_i. \end{aligned}$$

□

By rewriting (10) and (11) as

$$\phi = \left(y \prod_{i=1}^{r} \frac{1}{\tilde{\beta}_i} \prod_{i=1}^{r} \frac{\tilde{\beta}_i^2 y^2 - az}{z^2 - \tilde{\beta}_i y} \prod_{i=1}^{s} \frac{az - \beta_i\gamma_i y^2}{yz - \beta_i\gamma_i}, z \prod_{i=1}^{r} \frac{\tilde{\beta}_i}{\tilde{\beta}_i} \prod_{i=1}^{r} \frac{a - \tilde{\beta}_i yz}{z^2 - \tilde{\beta}_i y} \prod_{i=1}^{s} \frac{ay - \beta_i\gamma_i z^2}{yz - \beta_i\gamma_i}\right) \tag{12}$$
$$= \left(y \prod_{i=1}^{r} \tilde{\beta}_i \prod_{i=1}^{r} \frac{\tilde{\beta}_i y - z^2}{yz - \tilde{\beta}_i^2} \prod_{i=1}^{s} \frac{az - \beta_i\gamma_i y^2}{yz - \beta_i\gamma_i}, z \prod_{i=1}^{r} \tilde{\beta}_i \prod_{i=1}^{r} \frac{\tilde{\beta}_i z - y^2}{yz - \tilde{\beta}_i^2} \prod_{i=1}^{s} \frac{ay - \beta_i\gamma_i z^2}{yz - \beta_i\gamma_i}\right) \tag{13}$$

and straightforward counting as before, the costs of (12) and (13) are given in Table 1.

5.2 Projective coordinates

Corollary 3. *Let* $F = \mathcal{O} \cup \{(\tilde{\alpha}_i : \tilde{\beta}_i : \tilde{\beta}_i)\}_{i=1}^{r} \cup \{(\alpha_i : \beta_i : \gamma_i), (\alpha_i : \gamma_i : \beta_i)\}_{i=1}^{s}$ *be a subgroup of* $H(a, d)$ *and* $|F| \not\equiv 0 \pmod 3$, *where* $(\alpha_i : \beta_i : \gamma_i)$ *has order greater than 2 and* $(\tilde{\alpha}_i : \tilde{\beta}_i : \tilde{\beta}_i)$ *has order 2. Let* ϕ *be the isogeny in Theorem 4 with kernel* F. *Then,*

$$\begin{aligned}\phi = \Big(&X\prod_{i=1}^{r}\tilde{\beta}_i^2 XY - \tilde{\alpha}_i\tilde{\beta}_i Z^2\prod_{i=1}^{s}\alpha_i^2 YZ - \beta_i\gamma_i X^2 :\\ &Y\prod_{i=1}^{r} a\tilde{\alpha}_i^2 XZ - \tilde{\beta}_i^2 Y^2\prod_{i=1}^{s} a\alpha_i^2 XZ - \beta_i\gamma_i Y^2 :\\ &Z\prod_{i=1}^{r}\tilde{\beta}_i^2 YZ - a\tilde{\alpha}_i\tilde{\beta}_i X^2\prod_{i=1}^{s} a\alpha_i^2 XY - \beta_i\gamma_i Z^2\Big) \qquad (14)\\ = \Big(&X\prod_{i=1}^{r}\tilde{\alpha}_i^2 YZ - \tilde{\beta}_i^2 X^2\prod_{i=1}^{s}\alpha_i^2 YZ - \beta_i\gamma_i X^2 :\\ &Y\prod_{i=1}^{r}\tilde{\beta}_i^2 XY - \tilde{\alpha}_i\tilde{\beta}_i Z^2\prod_{i=1}^{s} a\alpha_i^2 XZ - \beta_i\gamma_i Y^2 :\\ &Z\prod_{i=1}^{r}\tilde{\beta}_i^2 XZ - \tilde{\alpha}_i\tilde{\beta}_i Y^2\prod_{i=1}^{s} a\alpha_i^2 XY - \beta_i\gamma_i Z^2\Big) \qquad (15)\end{aligned}$$

Proof. The corollary follows by projectivizing the expressions in previous corollaries. □

By straightforward counting, (15) takes $(2r+s)S + (r+s)M + sM_a$ to process the kernel and $(9s+9r+3)M + 3S$ for the input point, and (14) takes additional $2rM_a$ for processing the kernel. The results are summarized in Table 1.

Table 1: Computational cost of our isogeny formulas on twisted Hessian curves.

	Process kernel	Process input point
Z-affine (5)	$sS + rM + (r+2s)M_a$	$2S + (8s+5r+2)M + 1I$
Z-affine (6)	$(r+s)S + 2sM_a$	$2S + (8s+5r+2)M + 1I$
X-affine (12)	$rS + (r+s-1)M$	$2S + (6r+5s+4)M + 2M_a + 1I$
X-affine (13)	$rS + (r+s-1)M$	$2S + (5r+5s+4)M + 2M_a + 1I$
Projective (14)	$(2r+s)S + (r+s)M + (s+2r)M_a$	$3S + (9s+9r+3)M$
Projective (15)	$(2r+s)S + (r+s)M + sM_a$	$3S + (9s+9r+3)M$

Table 2: Comparison of the computational costs for various isogeny formulas. We denote by $cost(2^s)$ the cost of computing 2^s.

Formula	Process kernel	Process input point
twisted Hessian (Z-affine) [this work]	$0.8sM + 2sM_a$	$(8s+3.6)M + 1I$
twisted Hessian (X-affine) [this work]	$(s-1)M$	$(5s+5.6)M + 2M_a + 1I$
twisted Hessian (projective) [this work]	$1.8sM + sM_a$	$(9s+5.4)M$
Edwards (affine) [11] + [this work]	$(4.4s+0.8)M$	$(6s+2.6)M + 1I + cost(2^s)$
Edwards (projective) [11] + [this work]	$(8s+0.8)M$	$(7s+7.2)M + cost(2^s)$
Huff (affine) [11]	$(3.6s+1.6)M$	$(6s-0.4)M + 2I$
Vélu's [2]	$9.8M$	$(13s+1.8)M + 1I$

5.3 Comparison with other formulas

For comparison, consider the isogeny formula from [11] for Edwards curves, which is the most efficient to our knowledge so far. We note that the authors reported the cost of $(6s+1)M + 2S + I$ in affine coordinates or $(6s+3)M + 4S$ in mixed coordinates (the kernel is in affine coordinates and the input point is in projective coordinates), for computing an image point. However, in each case, up to sI were required for preprocessing the kernel points. Here, we consider a different approach that avoids inversions entirely in the projective case and uses only 1 inversion in the affine case. First, we consider the projective case. Suppose the kernel is

$$F = \{(0:1:1)\} \cup \{(\alpha_i : \beta_i : \gamma_i)\}_{i=1}^{s} \cup \{(-\alpha_i : \beta_i : \gamma_i)\}_{i=1}^{s}.$$

The isogeny is

$$\begin{aligned}(x:y:z) \mapsto \Big(& x \prod_{i=1}^{s} \beta_i^2 \gamma_i^4 x^2 z^2 - \alpha_i^2 \gamma_i^4 y^2 z^2 : \\ & y \prod_{i=1}^{s} \beta_i^2 \gamma_i^4 y^2 z^2 - \alpha_i^2 \gamma_i^4 x^2 z^2 : \\ & z \prod_{i=1}^{s} \beta_i^2 \gamma_i^4 z^4 - d^2 \alpha_i^2 \beta_i^4 x^2 y^2 \Big).\end{aligned}$$

For processing the kernel, one can compute $\beta_i^2\gamma_i^4$, $\alpha_i^2\gamma_i^4$, and $d^2\alpha_i^2\beta_i^4$, for all i, with $(5s+1)S + 4sM$. For computing the image point, x^2z^2, y^2z^2, x^2y^2, and z^4, take $3M$ and $4S$. If the characteristic is not 2, By the definition of (twisted) Edwards curves, the characteristic is not 2, and we can compute each pair of $2(\beta_i^2\gamma_i^4x^2z^2 - \alpha_i^2\gamma_i^4y^2z^2)$ and $2(\beta_i^2\gamma_i^4y^2z^2 - \alpha_i^2\gamma_i^4x^2z^2)$ for the x and y coordinates with only $2M$ using the identities:

$$\begin{aligned}2(ax - by) &= (a-b)(x+y) + (a+b)(x-y) \text{ and} \\ 2(ay - bx) &= (a-b)(x+y) - (a+b)(x-y).\end{aligned}$$

Each factor $\beta_i^2\gamma_i^4z^4 - d^2\alpha_i^2\beta_i^4x^2y^2$ in the z coordinate takes $2M$, and let $cost(2^s)$ be the cost of computing 2^s. Multiplication of all the factors in the x and y coordinates takes $2sM$, and multiplication of the factors in the z coordinate including 2^s takes $(s+1)M$. Therefore, the total cost of computing an image point is $4S + (7s+4)M + cost(2^s)$.

Similarly, in affine coordinates, we can compute the Edwards isogeny map

$$(x, y) \mapsto \left(x \prod_{i=1}^{s} \frac{\beta_i^2 x^2 - \alpha_i^2 y^2}{\beta_i^2 - d^2\alpha_i^2\beta_i^4 x^2 y^2}, y \prod_{i=1}^{s} \frac{\beta_i^2 y^2 - \alpha_i^2 x^2}{\beta_i^2 - d^2\alpha_i^2\beta_i^4 x^2 y^2} \right)$$

using $(3s+1)S + 2sM$ for processing the kernel and $(6s+1)M + 2S + I + cost(2^s)$ for the input point.

The comparison is summarized in Table 2, where we assume the kernel size is odd and $1S = 0.8M$. We note that our formulas for twisted Hessian curves have the lowest costs for processing the kernel and our X-affine formula has the lowest cost for processing an input point in affine coordinates.

6 Conclusion

In this work we looked at computing isogenies between elliptic curves represented as twisted Hessian curves. There still exist other models of curves for which direct isogeny formulas are not known, such as Jacobi quartics and Jacobi intersections [32, 33]. It would be interesting to see if simple isogeny formulas exist for these models. We note that the original Velu isogeny formulas are expressed as a sum, while the more recent Edwards, Hessian, and Montgomery formulas all involve a product of expressions involving the kernel points. Is there

a multiplicative version of Velu's formulas? Or additive expressions for isogenies of the alternate models of elliptic curves?

We leave it as future work to further optimize the formulas presented and integrate them into specific applications. For example, this could include efficient computation of low degree isogenies. Low-degree isogenies are used in post-quantum cryptographic isogeny schemes, and if optimized formulas can be found, they may lead to implementing these isogeny cryptosystems using twisted Hessian curves. In particular, it may be interesting to compute the 9-isogeny formulas for Hessian curves, similar to the work on 4-isogenies over Montgomery and Edwards models [19, 34].

It would also be interesting to use low degree isogenies to compute scalar multiplication formulas on Hessian curves for small scalars like 2, 3, and 5, as done in [35, 36], especially for curves with j-invariant zero.

References

[1] J. H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, Springer, 2nd ed., 2009.

[2] J. Vélu, "Isogénies entre courbes elliptiques," *CR Acad. Sci. Paris, Séries A*, vol. 273, pp. 305–347, 1971.

[3] P. L. Montgomery, "Speeding the Pollard and elliptic curve methods of factorization," *Mathematics of Computation*, vol. 48, no. 177, pp. 243–264, 1987.

[4] K. Okeya, H. Kurumatani, and K. Sakurai, "Elliptic curves with the Montgomery-form and their cryptographic applications," in *International Workshop on Public Key Cryptography*, pp. 238–257, Springer, 2000.

[5] H. Edwards, "A normal form for elliptic curves," *Bulletin of the American Mathematical Society*, vol. 44, no. 3, pp. 393–422, 2007.

[6] D. J. Bernstein and T. Lange, "Faster addition and doubling on elliptic curves," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 29–50, Springer, 2007.

[7] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, "Twisted Edwards curves," in *International Conference on Cryptology in Africa*, pp. 389–405, Springer, 2008.

[8] M. Joye, M. Tibouchi, and D. Vergnaud, "Huff's model for elliptic curves," in *International Algorithmic Number Theory Symposium*, pp. 234–250, Springer, 2010.

[9] H. Wu and R. Feng, "Elliptic curves in Huff's model," *Wuhan University Journal of Natural Sciences*, vol. 17, no. 6, pp. 473–480, 2012.

[10] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange, "Twisted Hessian curves," in *International Conference on Cryptology and Information Security in Latin America*, pp. 269–294, Springer, 2015.

[11] D. Moody and D. Shumow, "Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves," *Mathematics of Computation*, vol. 85, no. 300, pp. 1929–1951, 2016.

[12] C. Costello and H. Hisil, "A simple and compact algorithm for SIDH with arbitrary degree isogenies," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 303–329, Springer, 2017.

[13] J. Renes, "Computing isogenies between Montgomery curves using the action of (0, 0)," in *The Eighth International Conference on Post-Quantum Cryptography, PQCrypto*, pp. 229–247, Springer, 2017.

[14] T. Izu, J. Kogure, M. Noro, and K. Yokoyama, "Efficient implementation of Schoof's algorithm," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 66–79, Springer, 1998.

[15] R. Lercier and F. Morain, "Computing isogenies between elliptic curves over $\mathbb{F}_p^n$ using Couveignes's algorithm," *Mathematics of Computation*, vol. 69, no. 229, pp. 351–370, 2000.

[16] D. Jao, S. D. Miller, and R. Venkatesan, "Do all elliptic curves of the same order have the same difficulty of discrete log?," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 21–40, Springer, 2005.

[17] E. Teske, "An elliptic curve trapdoor system," *Journal of Cryptology*, vol. 19, no. 1, pp. 115–133, 2006.

[18] D. X. Charles, K. E. Lauter, and E. Z. Goren, "Cryptographic hash functions from expander graphs," *Journal of Cryptology*, vol. 22, no. 1, pp. 93–113, 2009.

[19] L. De Feo, D. Jao, and J. Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," *Journal of Mathematical Cryptology*, vol. 8, no. 3, pp. 209–247, 2014.

[20] N. P. Smart, "The Hessian form of an elliptic curve," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 118–125, Springer, 2001.

[21] H. Hisil, G. Carter, and E. Dawson, "New formulae for efficient elliptic curve arithmetic," in *International Conference on Cryptology in India*, pp. 138–151, Springer, 2007.

[22] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson, "Faster group operations on elliptic curves," in *Proceedings of the Seventh Australasian Conference on Information Security*, vol. 98, pp. 7–20, Australian Computer Society, Inc., 2009.

[23] E. Fouotsa, "Parallelizing pairings on Hessian elliptic curves," *Arab Journal of Mathematical Sciences*, vol. 25, no. 1, pp. 29 – 42, 2019.

[24] M. Joye and J.-J. Quisquater, "Hessian elliptic curves and side-channel attacks," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 402–410, Springer, 2001.
[25] R. R. Farashahi and M. Joye, "Efficient arithmetic on Hessian curves," in *International Workshop on Public Key Cryptography*, pp. 243–260, Springer, 2010.
[26] R. R. Farashahi, H. Wu, and C.-A. Zhao, "Efficient arithmetic on elliptic curves over fields of characteristic three," in *International Conference on Selected Areas in Cryptography*, pp. 135–148, Springer, 2012.
[27] D. Kohel, "The geometry of efficient arithmetic on elliptic curves," *Arithmetic, Geometry, Coding Theory and Cryptography*, vol. 637, pp. 95–109, 2015.
[28] D. Moody and H. Wu, "Families of elliptic curves with rational 3-torsion," *Journal of Mathematical Cryptology*, vol. 5, no. 3-4, pp. 225–246, 2012.
[29] L. C. Washington, *Elliptic curves: number theory and cryptography*. CRC press, 2008.
[30] T. S. Gustavsen and K. Ranestad, "A simple point counting algorithm for Hessian elliptic curves in characteristic three," *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, no. 2, pp. 141–150, 2006.
[31] W. Fulton, *Algebraic curves: An introduction to algebraic geometry*. 2008. http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf.
[32] O. Billet and M. Joye, "The Jacobi model of an elliptic curve and side-channel analysis," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (M. Fossorier, T. Høholdt, and A. Poli, eds.), (Berlin, Heidelberg), pp. 34–42, Springer Berlin Heidelberg, 2003.
[33] P. Y. Liardet and N. P. Smart, "Preventing SPA/DPA in ECC systems using the Jacobi form," in *Cryptographic Hardware and Embedded Systems — CHES 2001* (Ç. K. Koç, D. Naccache, and C. Paar, eds.), (Berlin, Heidelberg), pp. 391–401, Springer Berlin Heidelberg, 2001.
[34] S. Kim, K. Yoon, Y. Park, and S. Hong, "Optimized method for computing odd-degree isogenies on Edwards curves," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 273–292, Springer, 2019.
[35] C. Doche, T. Icart, and D. R. Kohel, "Efficient scalar multiplication by isogeny decompositions," in *International Workshop on Public Key Cryptography*, pp. 191–206, Springer, 2006.
[36] D. Moody, "Using 5-isogenies to quintuple points on elliptic curves," *Information Processing Letters*, vol. 111, no. 7, pp. 314–317, 2011.