Lower bound of costs of formulas to compute image curves of 3-isogenies in the framework of generalized Montgomery coordinates

Tomoki Moriya¹, Hiroshi Onuki², Yusuke Aikawa², and Tsuyoshi Takagi²

¹ Computer Science, University of Birmingham, UK t.moriya@bham.ac.uk
² Department of Mathematical Informatics, The University of Tokyo, Japan {onuki,aikawa,takagi}@mist.i.u-tokyo.ac.jp

Abstract. In 2022, Moriya, Onuki, Aikawa, and Takagi proposed a new framework named generalized Montgomery coordinates to treat onecoordinate type formulas to compute isogenies. This framework generalizes some already known one-coordinate type formulas of elliptic curves. Their result shows that a formula to compute image points under isogenies is unique in the framework of generalized Montogmery coordinates; however, a formula to compute image curves is not unique. Therefore, we have a question: What formula is the most efficient to compute image curves in the framework of generalized Montogmery coordinates? In this paper, we analyze the costs of formulas to compute image curves of 3-isogenies in the framework of generalized Montgomery coordinates. From our result, the lower bound of the costs is $1\mathbf{M} + 1\mathbf{S}$ as a formula whose output and input are in affine coordinates, $2\mathbf{S}$ as an affine formula whose output is projective, and $2\mathbf{M} + 3\mathbf{S}$ as a projective formula.

Keywords: isogeny-based cryptography; Vélu's formulas; elliptic curves; generalized Montgomery coordinates.

1 Introduction

Isogeny-based cryptography is one of the candidates for post-quantum cryptography that resists quantum computers. This cryptography is based on Isogeny Problem of elliptic curves. The main merit of using isogeny-based cryptosystems is that they can achieve enough security under short data sizes; however, they need a lot of computational costs. Every isogeny-based cryptosystem has isogeny computations in its heart. Therefore, how to compute isogenies between elliptic curves efficiently is one of the interesting research themes in both computational algebra and isogeny-based cryptography.

One useful method to compute isogenies on elliptic curves is to rely on onecoordinates type formulas such as formulas of x-coordinates of Montgomery curves [Ren18,CH17,MR18]. One-coordinates type formulas are based on Vélu's formulas [Vél71] and have been proposed in some different forms of elliptic curves

by individual researchers independently (*e.g.*, *w*-coordinates of Edwards curves [KYPH19], *w*-coordinates of Huff's curves [HZHL20,DKW20]).

In 2022, Moriya, Onuki, Aikawa, and Takagi proved that these one-coordinates type formulas come from the same framework named generalized Montgomery coordinates [MOAT22]. This paper showed that formulas to compute image curves of isogenies derived from generalized Montgomery coordinates are not unique; however, the differences arise from a division polynomial that is determined by the degree of the target isogeny. More precisely, if rational functions $\phi_1(\alpha, h)$ and $\phi_2(\alpha, h)$ are formulas to output image curves of ℓ -isogenies, then the difference $\phi_1 - \phi_2$ is a product of the ℓ th division polynomial and a rational function whose denominator cannot be divided by the ℓ th division polynomial. Naturally, the difference among formulas provides the difference in their computational costs. Thus, we have the following question:

What is the most efficient formula to compute image curves of isogenies in the framework of generalized Montgomery coordinates?

Formulas in the case of 3-isogenies can be described as follows:

$$-6h^{3} + \alpha h^{2} + 6h + (3h^{4} + 4\alpha h^{3} + 6h^{2} - 1)\frac{\varphi(\alpha, h)}{\phi_{2}(\alpha, h)}$$

where h is an indeterminate corresponding to a kernel of a 3-isogeny, α corresponding to a domain curve, and $\varphi(\alpha, h)$ and $\phi_2(\alpha, h)$ are polynomials in $\mathbb{Z}[\alpha, h]$. Therefore, we can theoretically find the most efficient formula to compute image curves of 3-isogenies by considering the above rational function.

1.1 Contribution

In this paper, we find the lower bound of the cost to compute image curves of 3-isogenies in the framework of generalized Montgomery coordinates. We define costs as numbers of multiplications and squarings, and describe the cost of a multiplications and b squarings as $a\mathbf{M} + b\mathbf{S}$. The formula

$$-6h^3 + \alpha h^2 + 6h$$

that was proposed in [Ren18] is one of the most efficient formulas in those whose input and output are in affine coordinates, and its cost is $1\mathbf{M} + 1\mathbf{S}$. As an affine formula whose outputs are in projective coordinates, the formula

$$(-27h^4 + 18h^2 + 1:4h)$$

is one of the most efficient formulas, and its cost is 2S. As a projective formula, the formula

$$\frac{-27h^4 + 18h^2 + 1}{4h} = (-27H^4 + 18H^2Z^2 + Z^4 : 4HZ^3)$$

that proposed in [CLN16] is one of the most efficient formulas, and its cost is $2\mathbf{M} + 3\mathbf{S}$.



Fig. 1. Propositions and lemmas to prove Theorem 9

The main part of this paper is the proof of the result of project formulas (Theorem 9). This proof composes of some propositions and lemmas. Lemma 7 shows that there is no formula of degree 2 or less. Proposition 11 is the proposition of the case that the degree of the formula is more than 4, Proposition 14 is that of the case that the degree of the formula is 3, and Proposition 16 is that of the case that the degree of the formula is 4. Moreover, we need some lemmas to prove Proposition 16. Figure 1 shows the outline of the relationship between these propositions and lemmas.

Organization. In Section 2, we introduce some mathematical concepts (isogenies and generalized Montgomery coordinates). Section 3 provides the lower bound of costs to compute image curves under 3-isogenies and formulas that can be computed in the lower bound cost. In Section 3.1, we give the setting of analysis. In Section 3.2, we analyze affine formulas, and in Section 3.3, we analyze projective formulas. Finally, we conclude this paper in Section 4.

2 Preliminaries

In this section, we introduce some knowledge about isogenies and generalized Montgomery coordinates. Refer to [Sil09] and [MOAT22] for more detail.

Let E_1, E_2 be elliptic curves. If a morphism $f: E_1 \to E_2$ is surjective and a group morphism, we call f an *isogeny*. From an elliptic curve E_1 and its finite subgroup G, Vélu's formulas output an elliptic curve E_2 and a separable isogeny $f: E_1 \to E_2$ with ker f = G [Vél71]. We often denote E_2 by E_1/G . If an isogeny f is a separable isogeny whose kernel is a cyclic group of order ℓ , we call f an ℓ -isogeny.

Let k be a field, and E an elliptic curve defined over k. A *coordinate* of an elliptic curve is a function $h: E \to \overline{k}$, where \overline{k} is the algebraic closure of k. Note

that a function can be treated as a map from E to the projective line $\mathbb{P}_{\overline{k}}^1$. Let P be a point in E. An affine coordinate of P is a value $h(P) \in \overline{k}$ for some coordinate h, and a projective coordinate of P is an element (H(P) : Z(P)) in $\mathbb{P}_{\overline{k}}^1$ for some coordinate $(H : Z) : E \to \mathbb{P}_{\overline{k}}^1$. One-coordinate type formulas are formulas in which all points are represented as images of one fixed coordinate.

Remark 1. The definition of coordinates may not be compatible with those in other papers. This definition is reasonable to consider one-coordinate type formulas of elliptic curves.

Let k be a field of characteristic other than 2. Let E be an elliptic curve over k, let \mathcal{G} be a finite subgroup of E, and let \mathcal{R} be a subset of E such that $\mathcal{R} = R_0 + \mathcal{G}$ for some $R_0 \in \frac{1}{2}\mathcal{G} \setminus \mathcal{G}$ (*i.e.*, $2R_0 \in \mathcal{G}$ and $R_0 \notin \mathcal{G}$). A generalized Montgomery coordinate of E with respect to \mathcal{G} and \mathcal{R} is a function $h_{\mathcal{G},\mathcal{R}} \colon E \to \overline{k}$ satisfying

div
$$h_{\mathcal{G},\mathcal{R}} = 2 \sum_{R \in \mathcal{R}} (R) - 2 \sum_{P \in \mathcal{G}} (P).$$

A normalized generalized Montgomery coordinate $h_{\mathcal{G},\mathcal{R}}$ is a generalized Montgomery coordinate such that $h_{\mathcal{G},\mathcal{R}}(P+R) = \frac{1}{h_{\mathcal{G},\mathcal{R}}(P)}$ for any $P \in E$ and $R \in \mathcal{R}$. Let R_1 be a point in E such that $2R_1 \in \mathcal{G}$ and $R_1 \notin \mathcal{G} \cup \mathcal{R}$. A generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}}$ is a value

$$\alpha_{h_{\mathcal{G},\mathcal{R}}} = -h_{\mathcal{G},\mathcal{R}}(R_1) - \frac{1}{h_{\mathcal{G},\mathcal{R}}(R_1)}.$$

Note that $\alpha_{h_{\mathcal{G},\mathcal{R}}}$ is determined only from $h_{\mathcal{G},\mathcal{R}}$. A generalized Montgomery coefficient can be regarded as a parameter of an elliptic curve. This is an analogy for the fact that a Montgomery coefficient can be regarded as a parameter of a Montgomery curve. For a generalized Montgomery coefficient, we have the following lemma:

Lemma 2 ([MOAT22, Proposition 21]). For any positive odd integer m, there exist polynomials $\Phi_m, \Psi_m \in \mathbb{Z}[\alpha, h]$ such that, for any elliptic curve E and any normalized generalized Montgomery coordinate $h_{\mathcal{G},\mathcal{R}}$, the following three properties hold:

- It holds that

$$h_{\mathcal{G},\mathcal{R}}(mP) = \frac{h_{\mathcal{G},\mathcal{R}}(P)\Phi_m^2(\alpha_{h_{\mathcal{G},\mathcal{R}}},h_{\mathcal{G},\mathcal{R}}(P))}{\Psi_m^2(\alpha_{h_{\mathcal{G},\mathcal{R}}},h_{\mathcal{G},\mathcal{R}}(P))}$$

- The highest-degree monomial of $\Phi_m(\alpha, h)$ in the variable h is $h^{\frac{m^2-1}{2}}$;
- The highest-degree monomial of $\Psi_m(\alpha, h)$ in the variable h is $m \cdot h^{\frac{m^2-1}{2}}$.

We call Ψ_m the *m*th division polynomial of generalized Montgomery coordinates. We denote it by ψ_m .

Let ℓ be an odd integer, Q a point in E of order ℓ , and $f: E \to E/\langle Q \rangle$ an ℓ -isogeny with ker $f = \langle Q \rangle$. Let $h_{\mathcal{G},\mathcal{R}}$ be a normalized generalized Montgomery

coordinate of E such that $gcd(\#\mathcal{G}, \ell) = 1$. Then, a function $h_{f(\mathcal{G}), f(\mathcal{R})}$ is a normalized generalized Montgomery coordinate of $E/\langle Q \rangle$, and it holds that

$$h_{f(\mathcal{G}),f(\mathcal{R})}(f(P)) = h_{\mathcal{G},\mathcal{R}}(P) \prod_{i=1}^{(\ell-1)/2} \left(\frac{h_{\mathcal{G},\mathcal{R}}(P)h_{\mathcal{G},\mathcal{R}}(iQ) - 1}{h_{\mathcal{G},\mathcal{R}}(P) - h_{\mathcal{G},\mathcal{R}}(iQ)} \right)^2.$$
(1)

This is a formula to compute ℓ -isogenies. For an integer ℓ , there is a rational function $\phi_1(\alpha, h)/\phi_2(\alpha, h)$ such that

$$\alpha_{h_{f(\mathcal{G}),f(\mathcal{R})}} = \frac{\phi_1(\alpha_{h_{\mathcal{G},\mathcal{R}}}, h_{\mathcal{G},\mathcal{R}}(Q))}{\phi_2(\alpha_{h_{\mathcal{G},\mathcal{R}}}, h_{\mathcal{G},\mathcal{R}}(Q))}$$

for all $(E, h_{\mathcal{G},\mathcal{R}}, Q)$ and $f: E \to E/\langle Q \rangle$ with ker $f = \langle Q \rangle$. This is a formula to compute image curves of ℓ -isogenies. More precisely, we can define "a formula to compute image curves of ℓ -isogenies" as follows:

Definition 3 (A formula to compute image curves of ℓ -isogenies).

Let ℓ be a positive integer. A formula to compute image curves of ℓ -isogenies is a rational function ϕ_1/ϕ_2 satisfying

$$\alpha_{h_{f(\mathcal{G}),f(\mathcal{R})}} = \frac{\phi_1(\alpha_{h_{\mathcal{G},\mathcal{R}}}, h_{\mathcal{G},\mathcal{R}}(Q))}{\phi_2(\alpha_{h_{\mathcal{G},\mathcal{R}}}, h_{\mathcal{G},\mathcal{R}}(Q))}$$

for all $(k, E, h_{\mathcal{G}, \mathcal{R}}, Q, f)$ such that:

- -k: a field of characteristic other than 2 and ℓ ,
- -E: an elliptic curve defined over k,
- $-h_{\mathcal{G},\mathcal{R}}$: a normalized generalized Montgomery coordinate with gcd (# \mathcal{G}, ℓ) = 1,
- -Q: a point in E of order ℓ ,
- -f: an ℓ -isogeny $f: E \to E/\langle Q \rangle$ with ker $f = \langle Q \rangle$.

We know there are some different formulas to compute image curves of ℓ -isogenies (*e.g.*, [Ren18] and [MR18]). The following theorem shows these differences come from division polynomials.

Theorem 4. Let ℓ be an odd prime. If two rational functions $\frac{\phi_1(\alpha,h)}{\phi_2(\alpha,h)}$ and $\frac{\phi_3(\alpha,h)}{\phi_4(\alpha,h)}$ are formulas to compute image curves of ℓ -isogenies, then it holds that

$$\frac{\phi_1(\alpha,h)}{\phi_2(\alpha,h)} - \frac{\phi_3(\alpha,h)}{\phi_4(\alpha,h)} = \psi_\ell(\alpha,h) \cdot \frac{\varphi_1(\alpha,h)}{\varphi_2(\alpha,h)}$$

where $\varphi_1, \varphi_2 \in \mathbb{Z}[\alpha, h]$ and $\varphi_2(\alpha_{h_{\mathcal{G},\mathcal{R}}}, h_{\mathcal{G},\mathcal{R}}(Q))) \neq 0$ for all $(E, h_{\mathcal{G},\mathcal{R}})$ with $gcd(\#\mathcal{G}, \ell) = 1$ and Q of order ℓ .

Proof. Combine [MOAT22, Theorem 10] and Definition 3.

3 Settings and affine formula

In this section, we explain the settings for analysis and analyze the computational costs of affine formulas to compute image curves of 3-isogenies.

3.1 Settings for analysis

From a formula in [CH17, Theorem 1], we have

$$\alpha_{h_{f(\mathcal{G}),f(\mathcal{R})}} = -6h_{\mathcal{G},\mathcal{R}}(Q)^3 + \alpha_{h_{\mathcal{G},\mathcal{R}}}h_{\mathcal{G},\mathcal{R}}(Q)^2 + 6h_{\mathcal{G},\mathcal{R}}(Q),$$

where Q is a point of order 3 in E. From [MOAT22, Example 1], the 3rd division polynomial of computational coordinates is

$$3h^4 + 4\alpha h^3 + 6h^2 - 1.$$

Therefore, Theorem 4 shows that if $\phi_1(\alpha, h)/\phi_2(\alpha, h)$ is a formula to compute image curves of 3-isogenies and $\phi_1, \phi_2 \in \mathbb{Z}[\alpha, h]$, then

$$\frac{\phi_1(\alpha,h)}{\phi_2(\alpha,h)} = -6h^3 + \alpha h^2 + 6h + (3h^4 + 4\alpha h^3 + 6h^2 - 1)\frac{\varphi(\alpha,h)}{\phi_2(\alpha,h)}$$
(2)

for some $\varphi \in \mathbb{Z}[\alpha, h]$. We try to get the lower bound of costs of these formulas.

In this paper, we define a cost of a formula as a number of multiplications and squarings. Because the effects of additions and subtractions are small, we ignore their costs. Moreover, because the effects of divisions are huge, we do not consider computational algorithms that involve divisions. We denote the cost of a times multiplications and b times squarings by $a\mathbf{M} + b\mathbf{S}$, and we assume that $1\mathbf{M} \ge 1\mathbf{S} \ge (2/3)\mathbf{M}$.

We can compute $a \times b$ by a - 1 times additions of b. In this paper, we do not take into account this kind of algorithms whose cost varies with input because it seems inefficient and is hard to be analyzed.

3.2 Affine formula

In this subsection, we discuss the costs of affine formulas defined as follows:

Definition 5 (Affine formulas). An affine formula is a formula whose input is given in an affine coordinate.

We have the following theorem.

Theorem 6. If all inputs are given in affine coordinates and $\alpha_{h_{f(\mathcal{G}),f(\mathcal{R})}}$ is output by an affine coordinate, the lower bound of costs of the formulas to compute the generalized Montgomery coefficient of the codomain of 3-isogenies is $1\mathbf{M} + 1\mathbf{S}$, and the following formula can be computed with this lower bound.

$$-6h^3 + \alpha h^2 + 6h.$$

If all inputs are given in affine coordinates and $\alpha_{h_{f(\mathcal{G}),f(\mathcal{R})}}$ is output by projective coordinates, the lower bound of costs of the formulas to compute codomains of 3-isogenies are 2**S**, and the following formula can be computed with this lower bound.

$$(-3(3h^2 - 1)^2 + 4:4h).$$

To prove this theorem, we introduce the following lemma.

Lemma 7. Let ϕ_1/ϕ_2 be an affine formula to compute codomains of 3-isogenies. Then deg $\phi_1 \ge 3$ or deg $\phi_2 \ge 3$.

Proof. Suppose that deg $\phi_1 < 3$ and deg $\phi_2 < 3$. It holds that

$$\phi_1(\alpha, h) - (3h^4 + 4\alpha h^3 + 6h^2 - 1)\varphi(\alpha, h) = (-6h^3 + \alpha h^2 + 6h)\phi_2(\alpha, h).$$

By comparing degrees of both sides of the equation, we have deg $\varphi \leq 1$. Since $\phi_2 \neq 0$, we have $\varphi \neq 0$. Moreover, considering the highest-degree terms of both sides, we get

$$\varphi(\alpha, h) = c_1(6h - \alpha) + c_2,$$

where $c_1, c_2 \in \mathbb{Z}$ and $c_1 \neq 0$. Since the highest-degree term of the left hand side is $c_1(6h - \alpha)(3h^4 + 4\alpha h^3)$, the highest-degree term of ϕ_2 is $c_1(3h^2 + 4\alpha h)$. Furthermore, since the coefficient of $\alpha^2 h^2$ of the left-hand side is 0, we have

$$\phi_2(\alpha, h) = c_1(3h^2 + 4\alpha h) + c_3h + c_4$$

where $c_3, c_4 \in \mathbb{Z}$. Terms of degree 4 of the left-hand side is $-c_2(3h^4 + 4\alpha h^3)$ while those of degree 4 of the right-hand side is $c_3h(-6h^3 + \alpha h^2)$. Therefore, $c_2 = c_3 = 0$. Hence, terms of degree 3 of the left-hand side is $-c_16h^2(6h-\alpha)$ while those of degree 3 of the right-hand side is $c_16h(3h^2 + 4\alpha h)h + c_4(-6h^3 + \alpha h^2)$. We have $c_1 = c_4 = 0$. This contradicts $\phi_2 \neq 0$. Therefore, it holds that deg $\phi_1 \geq 3$ or deg $\phi_2 \geq 3$.

We now show the proof of Theorem 6.

Proof of Theorem 6. From Lemma 7, we have deg $\phi_1 \geq 3$ or deg $\phi_2 \geq 3$. To compute terms of degree 3, we need at least $1\mathbf{M} + 1\mathbf{S}$ cost, and to compute those of degree 4, we need at least $2\mathbf{S}$ cost. It is easy to check that to compute terms of degree 5 or more, we need more cost than $1\mathbf{M} + 1\mathbf{S}$.

In the case that the generalized Montgomery coefficient is output by an affine coordinate, there are no formulas with the cost of $2\mathbf{S}$ for the following reason. Suppose that there is a formula with the cost of $2\mathbf{S}$. This formula can be represented by

$$-6h^3 + \alpha h^2 + 6h + c(3h^4 + 4\alpha h^3 + 6h^2 - 1), \tag{3}$$

where $c \in \mathbb{Z} \setminus \{0\}$. On the other hand, from the cost to compute this formula, we have that this formula can be represented by

$$c_1(c_2(c_3h+c_4\alpha+c_5)^2+c_6h+c_7\alpha+c_8)^2+c_9(c_3h+c_4\alpha+c_5)^2+c_{10}h+c_{11}\alpha+c_{12},$$

where $c_1, \ldots, c_{12} \in \mathbb{Z}$. Since there are no terms of degree 2 or more in the variable α in the formula (3), $c_4 = c_7 = 0$. However, there is the αh^3 term in the formula (3). This is a contradiction. Therefore, $1\mathbf{M} + 1\mathbf{S}$ is the lower bound of costs of formulas. The following formula can be computed with this lower bound.

$$-6h^3 + \alpha h^2 + 6h = h^2(-6h + \alpha) + 6h.$$

In the case that the generalized Montgomery coefficient is output by projective coordinates, the following formula can be computed with this lower bound.

 $((-6h^3 + \alpha h^2 + 6h)4h - (3h^4 + 4\alpha h^3 + 6h^2 - 1): 4h) = (-3(3h^2 - 1)^2 + 4: 4h).$ This completes the proof of Theorem 6.

4 Projective formula

In the previous section, we analyzed costs of the formulas in the case that all inputs are given in affine coordinates. However, when using the formulas in isogeny-based cryptography, all inputs and outputs are usually given in projective coordinates. Therefore, we need to analyze projective formulas.

4.1 Terminology

We define projective formulas as follows:

Definition 8 (Projective formulas). A project formula is a formula with input and output in projective coordinates.

If $(\phi_1(A, C, H, Z) : \phi_2(A, C, H, Z))$ is a projective formula, then there is an affine formula $\tilde{\phi}_1(\alpha, h)/\tilde{\phi}_2(\alpha, h)$ such that

$$\frac{\phi_1(A, C, H, Z)}{\phi_2(A, C, H, Z)} = \frac{\phi_1(A/C, H/Z)}{\tilde{\phi}_2(A/C, H/Z)}.$$

These are more complicated to analyze than affine formulas. For simplicity, we assume that all polynomials appearing in the computations are homogeneous in this paper. Note that there are computations in which non-homogeneous polynomials appear. For example, $4H^2Z = (H^2 + Z)^2 - (H^2 - Z)^2$. We think such computations are not efficient; however, it is an open problem whether, in the most efficient computation of formulas, nonhomogeneous polynomials do not appear.

Now, we have the following theorem.

Theorem 9. If all inputs are given in projective coordinates and $\alpha_{h_{f(\mathcal{G})f(\mathcal{R})}}$ is output by projective coordinates, the lower bound of costs of the formulas to compute codomains of 3-isogenies are $2\mathbf{M}+3\mathbf{S}$. Moreover, the following formula can be computed with the lower bound.

$$(-3(3H^2 - Z^2)^2 + 4Z^4 : 4HZ^3) = (-27H^4 + 18H^2Z^2 + Z^4 : 4HZ^3).$$

The main goal of this section is to prove this theorem. We separate the situation into three cases to prove it. Let ϕ_1/ϕ_2 be irreducible over \mathbb{Z} . The first case is of deg $\phi_1 = \text{deg } \phi_2 > 4$ (Proposition 11). The second case is of deg $\phi_1 = \text{deg } \phi_2 = 3$ (Proposition 14). The third case is of deg $\phi_1 = \text{deg } \phi_2 = 4$ (Proposition 16). Theorem 9 follows from these propositions by a straightforward. Therefore, we prove these propositions instead of proving Theorem 9.

Before proving, we define the following concept for convenience.

Definition 10 (Seed polynomials). The computations of formulas are performed as follows.



We call a homogeneous polynomial appearing after a multiplication or a squaring in the computation a seed polynomial (e.g., $u'_n, \ldots, u_n^{(m_n)}$ and $u'_{n/2}, \ldots, u_{n/2}^{(m_{n/2})}$ in the above diagram).

We can estimate the cost by the number of seed polynomials appearing in the computation. For example, the formula

$$(-27H^4 + 18H^2Z^2 + Z^4 : 4HZ^3)$$

can be computed in $2\mathbf{M} + 3\mathbf{S}$ as the follow diagram:

 $\begin{array}{cccc} \deg 1 & \deg 2 \\ H & H-Z & (H-Z)^2 & 9H^2-6HZ+Z^2 \\ Z & \xrightarrow{\mathbf{a}} H+Z \xrightarrow{\mathbf{S}} (H+Z)^2 \xrightarrow{\mathbf{a}} -3H^2-2HZ+Z^2 \\ A & 2H & (2H)^2 & 9H^2+6HZ+Z^2 \\ C & -3H^2+2HZ+Z^2 \end{array}$

 $\deg 4$

formula

$$\xrightarrow{\mathbf{M}} -27H^4 + 18H^2Z^2 - 8HZ^3 + Z^4 \xrightarrow{\mathbf{a}} 4(-27H^4 + 18H^2Z^2 + Z^4)$$
(4)
$$-27H^4 + 18H^2Z^2 + 8HZ^3 + Z^4 \qquad 16HZ^3$$

Polynomials $(H - Z)^2$, $(H + Z)^2$, $(2H)^2$, $-27H^4 + 18H^2Z^2 - 8HZ^3 + Z^4$ and $-27H^4 + 18H^2Z^2 + 8HZ^3 + Z^4$ are seed polynomials in this diagram.

4.2 Degree of formula > 4

We now prove the case that the degree of a projective formula is more than 4.

Proposition 11. Let $(\phi_1 : \phi_2)$ be a projective formula to compute image curves of 3-isogenies such that the degree of the formula is more than 4 (i.e., $\deg \phi_1 = \deg \phi_2 > 4$ and ϕ_1/ϕ_2 is irreducible over \mathbb{Z}), then the cost to compute this formula is $2\mathbf{M} + 3\mathbf{S}$ or more.

The proposition follows from the following lemma by a straightforward.

Lemma 12. Let $(\phi_1 : \phi_2)$ be a projective formula. If the highest degree of seed polynomials is 5 or more appearing in the least cost computation of $(\phi_1 : \phi_2)$, then at least 6 seed polynomials are needed to compute the formula.

Proof. Let n be the highest degree of seed polynomials in the computation of $(\phi_1 : \phi_2)$ with the least cost. In this proof, we show the following three claims:

Claim 1: There are at least two seed polynomials of degree *n*.

- **Claim 2:** There are at least two seed polynomials of degree n/2 or more and less than n.
- **Claim 3:** There are at least two seed polynomials of degree n/4 or more and less than n/2 if the number of seed polynomials of degree n/2 or more is 4.

Because $n \ge 5$, there is at least one seed polynomial of degree n/4 or more and less than n/2. Therefore, if these claims hold, we find at least six seed polynomials.

Claim 1. There is at least two seed polynomials of degree n.

Proof of Claim 1. Suppose that there is only one seed polynomial of degree n. We denote this polynomial by u_n . Note that we assume that there are no nonhomogeneous polynomials in the computation. From the definition of seed polynomials, all polynomials of degree n appearing in the computation are obtained by adding u_n 's. Therefore, if the final result of the computation is two polynomials of degree n, the result ϕ_1/ϕ_2 becomes a constant function. If the degree of the final result of the computation is less than n, since we cannot compute polynomials of degree n-1 or less from u_n , we have u_n is not needed in the computation. This contradicts that the computation we consider has the least cost. Therefore, there are at least two seed polynomials of degree n.

Claim 2. There are at least two seed polynomials of degree n/2 or more and less than n.

Proof of Claim 2. For computing seed polynomials of degree n, we need at least one seed polynomial of degree n/2 or more and less than n. Suppose that there is only one seed polynomial of degree n/2 or more and less than n. We denote this seed polynomial by $u_{n/2}$. It is easy to see that all seed polynomials of degree n should be $cu_{n/2}^2$ or $v \cdot u_{n/2}$, where $c \in \mathbb{Z}$ and v is a polynomial of degree less than n/2. Therefore, we compute $(\phi'_1 u_{n/2} : \phi'_2 u_{n/2}) = (\phi_1 : \phi_2)$ for some ϕ'_1 and ϕ'_2 . However, we can compute $cu_{n/2}$ more efficiently than $cu_{n/2}^2$, and compute vmore efficiently than $v \cdot u_{n/2}$. Hence, we can compute $(\phi'_1 : \phi'_2)$ more efficiently than $(\phi'_1 u_{n/2} : \phi'_2 u_{n/2})$. This contradicts that the computation we consider has the least cost. Therefore, we need at least two seed polynomials of degree n/2or more and less than n.

Claim 3. There are at least two seed polynomials of degree n/4 or more and less than n/2 if the number of seed polynomials of degree n/2 or more is 4.

Proof of Claim 3. From Claim 1 and 2, there are two seed polynomials of degree n and two seed polynomials of degree n/2 or more and less than n. Suppose that there is only one seed polynomial of degree n/4 or more and less than n/2. We denote this seed polynomial by $u_{n/4}$. Let $u_{n/2}$ and $u'_{n/2}$ be seed polynomials of degree n/2 or more and less than n/2.

Here we have the following two cases:

Case 1: $\deg u_{n/2} < \deg u'_{n/2}$.

Case 2: $\deg u_{n/2} = \deg u'_{n/2}$.

We find contradictions in both cases.

Case 1: We have the following four cases:

$$(u_{n/2}, u'_{n/2}) = \begin{cases} (v \cdot u_{n/4}, v' \cdot u_{n/4}) \\ (v \cdot u_{n/4}, cu^2_{n/4}) \\ (v \cdot u_{n/4}, c(v \cdot u_{n/4})^2) \\ (cu^2_{n/4}, v' \cdot u^2_{n/4}) \end{cases}$$

where $c \in \mathbb{Z}$, and v and v' are polynomials of degree less than n/4. Since $\deg u_{n/2} < \deg u'_{n/2}$, we have $\deg (u_{n/2} \cdot u'_{n/2}) > n$ and $\deg u'^2_{n/2} > n$, and we do not compute $u_{n/2} \pm u'_{n/2}$. Hence, the seed polynomials of degree n are $du^2_{n/2}$, $w \cdot u_{n/2}$, or $w' \cdot u'_{n/2}$, where $d \in \mathbb{Z}$, and w and w' are polynomials of degree less than n/2. Therefore, seed polynomials of degree n have the one of following forms:

$$\begin{aligned} d(v \cdot u_{n/4})^2, \quad d(cu_{n/4}^2)^2, \quad w \cdot (v \cdot u_{n/4}), \quad w \cdot (cu_{n/4}^2), \\ w' \cdot (v' \cdot u_{n/4}), \quad w' \cdot c(v \cdot u_{n/4}^2), \quad w' \cdot (v' \cdot u_{n/4}^2). \end{aligned}$$
(5)

Since these are divisible by $u_{n/4}$, we can instead compute

$$d(v^{2} \cdot u_{n/4}), \quad d(c^{2}u_{n/4}^{3}), \quad w \cdot v, \quad w \cdot (cu_{n/4}), \\ w' \cdot v', \quad w' \cdot c(v \cdot u_{n/4}), \quad w' \cdot (v' \cdot u_{n/4}).$$
(6)

We can compute these polynomials except for the first two polynomials more efficiently than corresponding polynomials in (5) respectively. The first polynomial $d(v^2 \cdot u_{n/4})$ is computed in the same cost as $d(v \cdot u_{n/4})^2$; however, we need to compute a polynomial except for the first two polynomials in (6) in the case in which the first polynomial appears. Therefore, we can also compute polynomials more efficiently in this case. The second polynomial $d(c^2u_{n/4}^3)$ is computed less efficiently than $d(cu_{n/4}^2)^2$. In the case in which the second polynomial appears, we have $(u_{n/2}, u'_{n/2}) = (cu_{n/4}^2, v' \cdot u_{n/4}^2)$. Therefore, the seed polynomials of degree n are $d(cu_{n/4}^2)^2$ and $w' \cdot (v' \cdot u_{n/4}^2)$. Since both of them are divisible by $u_{n/4}^2$, we can instead compute $dc^2u_{n/4}^2$ and $w' \cdot v'$. We can compute these more efficiently than $d(cu_{n/4}^2)^2$ and $w' \cdot (v' \cdot u_{n/4}^2)$. Consequently, we find the more efficient way to compute seed polynomials of degree n in each case. This is a contradiction.

Case 2: We have the following two cases:

$$(u_{n/2}, u'_{n/2}) = \begin{cases} (v \cdot u_{n/4}, v' \cdot u_{n/4}) \\ (cu_{n/4}^2, c'u_{n/4}^2) \end{cases}$$

where $c, c' \in \mathbb{Z}$, and v and v' are polynomials of degree less than n/4. The seed polynomials of degree n are $(du_{n/2}+d'u'_{n/2}) \cdot (eu_{n/2}+e'u'_{n/2})$ or $(du_{n/2}+d'u'_{n/2})^2$, where $d, d', e, e' \in \mathbb{Z}$. If $(u_{n/2}, u'_{n/2}) = (cu^2_{n/4}, c'u^2_{n/4})$, then ϕ_1/ϕ_2 is a constant. This is a contradiction. If $(u_{n/2}, u'_{n/2}) = (v \cdot u_{n/4}, v' \cdot u_{n/4})$, then a seed polynomial of degree n is $(dv \cdot u_{n/4} + d'v' \cdot u_{n/4})^2$ or

 $(dv \cdot u_{n/4} + d'v' \cdot u_{n/4}) \cdot (ev \cdot u_{n/4} + e'v \cdot u_{n/4})$. We can instead compute $(dv + d'v')^2$ or $(dv + d'v') \cdot (ev + e'v)$, and these are more efficient. This is a contradiction.

Contradictions in both cases complete the proof of Claim 3. \Box

As mentioned in the first paragraph, from Claim 1, 2, and 3, there are at least 6 seed polynomials in the computation. This completes the proof of Lemma 12. $\hfill \Box$

Lemma 12 is not only for Proposition 11. As the diagram (4), the result of the computation is not needed to be irreducible. It is because the outputs of the computation are in projective coordinates. Therefore, there is a possibility that the degree of polynomials output is higher than deg ϕ_1 . Lemma 12 also covers most such cases. We give the following lemma that follows from Lemma 12 for simplicity.

Lemma 13. Let $(\phi_1 : \phi_2)$ be a projective formula. If the highest degree of seed polynomials appearing in the computation of $(\phi_1 : \phi_2)$ is 5 or more, then the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more regardless of the degree of the formula.

4.3 Degree of formula = 3

In this subsection, we prove the case that the degree of the formula is 3.

Proposition 14. Let $(\phi_1 : \phi_2)$ be a projective formula to compute image curves of 3-isogenies such that the degree of the formula is 3 (i.e., $\deg \phi_1 = \deg \phi_2 = 3$ and ϕ_1/ϕ_2 is irreducible over \mathbb{Z}), then it holds that

$$(\phi_1:\phi_2) = (27AH^2 + AZ^2 + 48CHZ: 4AHZ + 3CH^2 + 9CZ^2).$$

Moreover, the cost to compute this formula is $2\mathbf{M} + 3\mathbf{S}$ or more.

Proof. Let $\tilde{\phi}_1(\alpha, h)/\tilde{\phi}_2(\alpha, h)$ be an affine formula corresponding to $(\phi_1 : \phi_2)$. Remind the equation (2), and define a polynomial φ as in (2). Since deg $\tilde{\phi}_1 \leq 3$ and deg $_{\alpha} \tilde{\phi}_2 + \deg_h \tilde{\phi}_2 \leq 3$, it holds that

$$\phi_2(\alpha, h) = c_1(3h + 4\alpha)h + c_2\alpha + c_3h + c_4,$$

where $c_1, \ldots, c_4 \in \mathbb{Z}$. Moreover, we have

$$\varphi(\alpha, h) = c_1(6h - \alpha) + c_5,$$

where $c_5 \in \mathbb{Z}$. By definition of φ , it holds that

$$\tilde{\phi}_1(\alpha, h) = (-6h^3 + \alpha h^2 + 6h)\tilde{\phi}_2 + (3h^4 + 4\alpha h^3 + 6h^2 - 1)\varphi.$$
(7)

The terms of degree 4 of the right-hand side of (7) are

$$(-6c_3 + 3c_5)h^4 + (-6c_2 + c_3 + 4c_5)\alpha h^3 + c_2\alpha^2 h^2.$$

Therefore, $c_2 = c_3 = c_5 = 0$. The terms of degree 3 of the right-hand side of (7) are

$$(18c_1 - 6c_4 + 36c_1)h^3 + (24c_1 + c_4 - 6c_1)\alpha h^2.$$

Since $\max \{ \deg_{\alpha} \tilde{\phi}_1, \deg_{\alpha} \tilde{\phi}_2 \} + \max \{ \deg_h \tilde{\phi}_1, \deg_h \tilde{\phi}_2 \} \le 3$, we have $c_4 = 9c_1$ or $c_1 = c_4 = 0$. Therefore, it holds that

$$\frac{\tilde{\phi}_1(\alpha,h)}{\tilde{\phi}_2(\alpha,h)} = \frac{27\alpha h^2 + \alpha + 48h}{3h^2 + 4\alpha h + 9}$$

Hence, the only formula of degree 3 is

$$(\phi_1:\phi_2) = (27AH^2 + AZ^2 + 48CHZ: 4AHZ + 3CH^2 + 9CZ^2).$$

We now consider the cost to compute this formula. Note that it holds that $\deg \phi_1 = \deg \phi_2 \ge 3$ from Lemma 7. We only need to consider the cases that the highest degree of seed polynomials appearing in the computation is 3 or 4 from Lemma 13. By the same discussion as in the proof of Claim 2 in Lemma 12, there are two different seed polynomials of degree 2. Since there are two different seed polynomials of degree 3 or more, if the number of seed polynomials of degree 2 is four or more, then the cost of the computation is more than $2\mathbf{M}+3\mathbf{S}$. Therefore, we only need to consider the following two cases:

- a) There are two seed polynomials of degree 2.
- b) There are three seed polynomials of degree 2.

a) Two seed polynomials of degree 2:

Denote seed polynomials of degree 2 by u'_2 and u''_2 . The important fact to estimate the cost is that for any $(c_1, c_2) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, the rational function

$$\frac{c_1 27H^2 + c_1 Z^2 - 48c_2 HZ}{4c_1 HZ - 3c_2 H^2 - 9c_2 Z^2} \tag{8}$$

is irreducible over \mathbb{Z} (Lemma 15).

We consider the following two cases:

Case 1: $\deg_A u'_2 = \deg_A u''_2 = 0.$ **Case 2:** $\deg_A u'_2 > 0$ or $\deg_A u''_2 > 0$.

Case 1: Since ϕ_1 and ϕ_2 have terms of degree 1 in the variable A, we need to multiply a polynomial of degree 1 in the variable A in the computation. Therefore, there is a seed polynomial of degree 3. We denote this seed polynomial by u'_3 , and denote the polynomial of degree 1 used to compute u'_3 by $c_1A + c_2C + c_3H + c_4Z$, where $c_1 \neq 0$ and c_1, \ldots, c_4 are integers. By substituting $c_1A = -(c_2C + c_3H + c_4Z)$, we can get rid of u'_3 from the results of the computation. If this operation reduces the degree of ϕ_1/ϕ_2 , considering the H^3 and Z^3 terms leads to $c_3 = c_4 = 0$. Moreover, from the fact that (8) is irreducible, the reduced degree of ϕ_1/ϕ_2 is 2 or more. We suppose that the highest degree of seed polynomials is 3, and the number of seed polynomials of degree 3 is only 2. We denote these seed polynomials by u'_3 and u''_3 . It is clear that $\phi_1 = d_1 u'_3 + d_2 u''_3$ and $\phi_2 = d_3 u'_3 + d_4 u''_3$ for some $d_1, \ldots, d_4 \in \mathbb{Z}$. Therefore, erasing u'_3 decreases the degree of ϕ_1/ϕ_2 to 0. This is a contradiction. Hence, if the highest degree of seed polynomials is 3, the number of these seed polynomials is at least 3. In this case, the cost of the computation is $3\mathbf{M} + 2\mathbf{S}$ or more. If the highest degree of seed polynomials is 4, the cost of the computation is at least $2\mathbf{M} + 3\mathbf{S}$ as the following diagram.

Case 2: We fix $\deg_A u'_2 > 0$, and denote the polynomial of degree 1 used to compute u'_2 by $c_1A + c_2C + c_3H + c_4Z$, where $c_1 \neq 0$ and c_1, \ldots, c_4 are integers. In this case, we can erase u'_2 in the computation by substituting $c_1A = -(c_2C + c_3H + c_4Z)$. If u''_2 is also vanished by this operation, the results of the computation are

$$(c_1A + c_2C + c_3H + c_4Z)\phi_1, \quad (c_1A + c_2C + c_3H + c_4Z)\phi_2.$$

Therefore, the highest degree of seed polynomial should be 4. Suppose that there is no seed polynomial of degree 3. In this case, all seed polynomials of degree 4 can be represented by $d_1u_2'^2 + d_2u_2'u_2'' + d_3u_2''^2$. This is a contradiction since it can be divided by $(c_1A + c_2C + c_3H + c_4Z)^2$. Therefore, we have there is at least one seed polynomial of degree 3, and the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more as (9). For this reason, we can assume that u_2'' will not be erased by this operation. If the highest degree of seed polynomials is 3, all seed polynomials of degree 3 can be represented by $v(d_1u_2' + d_2u_2'')$, where v is a polynomial of degree 1, and $d_1, d_2 \in \mathbb{Z}$. Therefore, erasing u_2' always decreases the degree of ϕ_1/ϕ_2 to 1 or less. This contradicts the same discussion in Case 1. We next consider the case that the highest degree of seed polynomials is 4. Suppose that there are no seed polynomials of degree 3. Here, all seed polynomials of degree 4 are represented by

 $(d_1u'_2 + d_2u''_2)(d_3u'_2 + d_4u''_2)$, where $d_1, \ldots, d_4 \in \mathbb{Z}$. Therefore, erasing u'_2 decreases the degree of ϕ_1/ϕ_2 to 0. This is a contradiction. Hence, there is

at least one seed polynomial of degree 3, and the cost of the computation, in this case, is $2\mathbf{M} + 3\mathbf{S}$ or more.

Consequently, the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more if there are two seed polynomials of degree 2.

b) Three seed polynomials of degree 2:

Denote seed polynomials of degree 2 by u'_2 , u''_2 , and u'''_2 . If the highest degree of seed polynomials is 3, the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more because we need a multiplication to compute a seed polynomial of degree 3. We suppose that the highest degree of seed polynomials is 4. Note that we do not need to consider the case that there are seed polynomials of degree 3 as (9). Denote two seed polynomials of degree 4 by u'_4 and u''_4 . Now, we prove the following claim:

Claim 4. Both u'_4 and u''_4 are computed by multiplications.

If this claim holds, we need at least two multiplications. Therefore, the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more.

Proof of Claim 4. Suppose that u'_4 is computed by a squaring, and let $u'_4 = (e_1u'_2 + e_2u''_2 + e_3u'''_2)^2$ for $e_1, e_2, e_3 \in \mathbb{Z}$. We focus on terms of degree 2 in the variable A of u'_4 and u''_4 .

If u'_4 and u'_4 have terms of degree 0, 3 or 4 in the variables A and C, then the results of the computation are $d_3(d_1u'_4 + d_2u''_4)$ and $d_4(d_1u'_4 + d_2u''_4)$ for some $d_1, \ldots, d_4 \in \mathbb{Z}$, since we need to cancel terms of degree 0, 3 or 4 in the variables A and C. However, this is a contradiction because ϕ_1/ϕ_2 becomes a constant map. Therefore, u'_4 and u''_4 have no terms of degree 0, 3, and 4 in the variables A and C.

Therefore, it holds that $e_1u'_2 + e_2u''_2 + e_3u''_2$ is a polynomial of degree 1 in the variables A and C. It is because if not, u'_4 has terms of degree 0 or 4 in the variables A and C. Hence, we have the following two cases:

Case 1: u'_4 has terms of degree 2 in the variable A.

- **Case 2:** u'_4 has no terms of degree 2 in the variable A and has terms of degree 2 in the variable C.
- **Case 1:** Terms divisible by A^2 of u'_4 can be represented by $c_3A^2(c_1H + c_2Z)^2$ for some $c_1, c_2, c_3 \in \mathbb{Z} \setminus \{0\}$. In this case, terms divisible by A^2 of u''_4 can be represented by $c_5A^2(c_1^2H^2 + c_4HZ + c_2^2Z^2)$ for some $c_4, c_5 \in \mathbb{Z} \setminus \{0\}$ since 4AHZ is the only term of ϕ_2 of degree 1 in the variable A. By considering the terms divisible by A^2 of ϕ_1 , we have

$$c_4c_3A^2(c_1H+c_2Z)^2 - 2c_1c_2c_5A^2(c_1^2H^2+c_4HZ+c_2^2Z^2) = c(27A^2H^2+A^2Z^2)$$

for some $c \in \mathbb{Z}$. By comparing coefficients of both sides of A^2H^2 and A^2Z^2 terms, we have $(c_1/c_2)^2 = 27$. This contradicts $c_1, c_2 \in \mathbb{Z}$.

Case 2: Terms divisible by C^2 of u'_4 can be represented by $c_3C^2(c_1H + c_2Z)^2$ and those of u''_4 can be represented by $c_5C^2(c_1^2H^2 + c_4HZ + c_2^2Z^2)$ for some $c_1, \ldots, c_5 \in \mathbb{Z} \setminus \{0\}$ for the similar reason as in Case 1. We have

$$c_4c_3C^2(c_1H+c_2Z)^2-2c_1c_2c_5C^2(c_1^2H^2+c_4HZ+c_2^2Z^2)=c(3C^2H^2+9C^2Z^2)$$

for some $c \in \mathbb{Z}$. By seeing the $C^2 H^2$ and $C^2 Z^2$ terms, we have $(c_2/c_1)^2 = 3$. This contradicts $c_1, c_2 \in \mathbb{Z}$.

The above discussions complete the proof of Claim 4.

Hence, the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more if there are three seed polynomials of degree 2.

Consequently, the cost of the formula computation is $2\mathbf{M} + 3\mathbf{S}$ or more. This completes the proof of Proposition 14.

Lemma 15. For any $(c_1, c_2) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, the rational function

$$\frac{c_1 27H^2 + c_1 Z^2 - 48c_2 HZ}{4c_1 HZ - 3c_2 H^2 - 9c_2 Z^2}$$

is irreducible over \mathbb{R} .

Proof. Since

$$\frac{c_1 27H^2 + c_1 Z^2}{-3c_2 H^2 - 9c_2 Z^2}$$

is not constant for all $(c_1, c_2) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, the given rational function in the lemma is not constant for all $(c_1, c_2) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

Suppose that there is a polynomial $d_1H + d_2Z \in \mathbb{R}[H, Z]$ such that $c_127H^2 + c_1Z^2 - 48c_2HZ$ and $4c_1HZ - 3c_2H^2 - 9c_2Z^2$ is divisible by $d_1H + d_2Z$ for some $c_1, c_2 \in \mathbb{Z} \setminus \{(0,0)\}$. If $d_1 = 0$, then $c_1 = c_2 = 0$. This is a contradiction, and we have $d_1 \neq 0$. Put $r = -d_2/d_1$. We substitute H = rZ into the rational function. Then we get

$$c_1 27r^2 + c_1 - 48c_2r = 0, \quad 4c_1r - 3c_2r^2 - 9c_2 = 0.$$

We have

$$\begin{pmatrix} 27r^2 + 1 & -48r \\ 4r & -3r^2 - 9 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Since $(c_1, c_2) \neq (0, 0)$, it holds that

$$(27r^{2}+1)(-3r^{2}-9) - (-48r)(4r) = -9(3r^{2}+1)^{2} = 0$$

This contradicts $r \in \mathbb{R}$. This completes the proof of Lemma 15.

Lower bound of costs to compute image curves of 3-isogenies 17

4.4 Degree of formula = 4

In this subsection, we prove the case that the degree of the formula is 4.

Proposition 16. Let $(\phi_1 : \phi_2)$ be a projective formula to compute image curves of 3-isogenies such that the degree of the formula is 4 (i.e., $\deg \phi_1 = \deg \phi_2 = 4$ and ϕ_1/ϕ_2 is irreducible over \mathbb{Z}), then the cost to compute this formula is $2\mathbf{M}+3\mathbf{S}$ or more. Moreover, the following formula can be computed with the lower bound.

 $(-3(3H^2 - Z^2)^2 + 4Z^4 : 4HZ^3) = (-27H^4 + 18H^2Z^2 + Z^4 : 4HZ^3).$

To prove this proposition, we consider the following three cases. The first case is of $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 = 2$ (Lemma 18), the second case is of $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 = 1$ (Lemma 19), and the final case is of $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 = 0$ (Lemma 20). Because Lemma 17 shows that $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 \leq 2$, Proposition 16 follows from these three lemmas by a straightforward.

We now prove the four lemmas for Proposition 16.

Lemma 17. Let $(\phi_1 : \phi_2)$ be a projective formula to compute image curves of 3-isogenies such that the degree of the formula is 4 (i.e., $\deg \phi_1 = \deg \phi_2 = 4$ and ϕ_1/ϕ_2 is irreducible over \mathbb{Z}), and let $\tilde{\phi}_1(\alpha, h)/\tilde{\phi}_2(\alpha, h)$ be an affine formula corresponding to $(\phi_1 : \phi_2)$. Then $\deg_{\alpha} \tilde{\phi}_1$ and $\deg_{\alpha} \tilde{\phi}_2$ are 2 or less.

Proof. If deg $\tilde{\phi}_2 < 2$, it is easy to see that deg_{α} $\tilde{\phi}_1$, deg_{α} $\tilde{\phi}_2 \leq 2$. We can assume deg $\tilde{\phi}_2 \geq 2$. Remind the equation (2). Since the terms of degree 5 or more in $\tilde{\phi}_1$ are deleted, the highest degree terms of $\tilde{\phi}_2$ have $h(3h+4\alpha)$ as a factor. Therefore, it holds that deg_h $\tilde{\phi}_2 \geq 2$. Since

$$\max \{ \deg_{\alpha} \tilde{\phi}_1, \deg_{\alpha} \tilde{\phi}_2 \} + \max \{ \deg_h \tilde{\phi}_1, \deg_h \tilde{\phi}_2 \} = 4$$

we have $\deg_{\alpha} \tilde{\phi}_1, \deg_{\alpha} \tilde{\phi}_2 \leq 2$.

Lemma 18. Let $(\phi_1 : \phi_2)$ be a projective formula to compute image curves of 3-isogenies such that the degree of the formula is 4 (i.e., $\deg \phi_1 = \deg \phi_2 = 4$ and ϕ_1/ϕ_2 is irreducible over \mathbb{Z}). If $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 = 2$, the cost to compute this formula is $2\mathbf{M} + 3\mathbf{S}$ or more.

Proof. Let $\phi_1(\alpha, h)/\phi_2(\alpha, h)$ be an affine formula corresponding to $(\phi_1 : \phi_2)$. As we have already seen, there is a polynomial $\varphi(\alpha, h) \in \mathbb{Z}[\alpha, h]$ such that

$$\frac{\phi_1}{\tilde{\phi}_2} = -6h^3 + \alpha h^2 + 6h + (3h^4 + 4\alpha h^3 + 6h^2 - 1)\frac{\varphi}{\tilde{\phi}_2}$$

Note that $\deg_h \tilde{\phi}_2 \leq 2$ because $\deg_{H,Z} \phi_2 = 2$. Since $\deg \tilde{\phi}_1 \leq 4$, polynomials φ and $\tilde{\phi}_2$ can be represented by

$$\phi_2(\alpha, h) = (3h + 4\alpha)h(c_1\alpha + c_2) + c_4\alpha + c_5h + c_6, \varphi(\alpha, h) = (6h - \alpha)(c_1\alpha + c_2) + c_3,$$

where $c_1, \ldots, c_6 \in \mathbb{Z}$. As $\deg_h \tilde{\phi}_1 \leq 2$, a forceful calculation leads to

$$c_3 = 4c'_5, \quad c_4 = 9c_1 + 3c'_5, \quad c_5 = 2c'_5, \quad c_6 = 9c_2,$$

where $c'_5 \in \mathbb{Z}$. Therefore, we have

 ϵ

$$\begin{aligned} \varphi(\alpha,h) &= (6h-\alpha)(c_1\alpha+c_2) + 4c_5', \end{aligned} \tag{10} \\ \tilde{\phi}_1(\alpha,h) &= (27c_1+3c_5')\alpha^2h^2 + c_1\alpha^2 + 27c_2\alpha h^2 \\ &\quad + 36c_5'h^2 + (18c_5'+48c_1)\alpha h + c_2\alpha + 48c_2h - 4c_5', \end{aligned} \tag{11}$$

$$\phi_2(\alpha, h) = (3h + 4\alpha)h(c_1\alpha + c_2) + (9c_1 + 3c_5')\alpha + 2c_5'h + 9c_2.$$
(12)

From Lemma 13, we only consider the case that the highest degree of seed polynomials appearing in the computation is 4. By the discussion in the proof of Lemma 12, there are two different seed polynomials of degree 2. Since there are at least two different seed polynomials of degree 4, if the number of seed polynomials of degree 2 is four or more, then the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more. Hence, we only need to consider the following cases:

- a) There are two seed polynomials of degree 2.
- b) There are three seed polynomials of degree 2.

a) Two seed polynomials of degree 2:

We denote seed polynomials of degree 2 by u'_2 and u''_2 . We now prove that there is at least one seed polynomial of degree 3. If so, then the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more, as the diagram (9).

Suppose that there is no seed polynomial of degree 3 in the computation. In this case, ϕ_1 and ϕ_2 can be represented by $d_1u_2'^2 + d_2u_2'u_2'' + d_3u_2''^2$ for some $d_1, d_2, d_3 \in \mathbb{Z}$. Put $\tilde{u}_2'(\alpha, h) = u_2'(\alpha, 1, h, 1)$, and $\tilde{u}_2''(\alpha, h) = u_2''(\alpha, 1, h, 1)$. Then, $\tilde{\phi}_1$ and $\tilde{\phi}_2$ are represented by

$$\tilde{\phi}_1 = d'_1 \tilde{u}_2'^2 + d'_2 \tilde{u}_2' \tilde{u}_2'' + d'_3 \tilde{u}_2'^2,
\tilde{\phi}_2 = d''_1 \tilde{u}_2'^2 + d''_2 \tilde{u}_2' \tilde{u}_2'' + d''_3 \tilde{u}_2''^2,$$
(13)

for some $d'_1, d'_2, d'_3, d''_1, d''_2, d''_3 \in \mathbb{Z}$.

Polynomials \tilde{u}'_2 and \tilde{u}''_2 are not constant for the following reason. Suppose that \tilde{u}'_2 is a constant. Then we have deg $\tilde{u}''_2 = 2$ from Lemma 7 and the equations (13). Therefore, we have $d''_3 = 0$ and deg $\tilde{\phi}_2 \leq 2$ because the polynomial $\tilde{\phi}_2$ has no terms of $\alpha^2 h^2$, h^4 , and α^4 from the equation (12). This derives $c_1 = 0$. As $\tilde{\phi}_1$ has no term of h^4 , the equations (13) show that there is no term of h^2 in \tilde{u}''_2 and $\tilde{\phi}_2$. Hence, we have $c_2 = 0$ and deg $\tilde{\phi}_2 \leq 1$. Since deg $\tilde{u}''_2 = 2$, it holds that $d''_2 = 0$ and $c'_5 = 0$. However, this is a contradiction because $\tilde{\phi}_1 = \tilde{\phi}_2 = 0$ if $c_1 = c_2 = c'_5 = 0$.

Since $\max \{ \deg_A \phi_1, \deg_A \phi_2 \} = 2$, we have $\deg_A u'_2 \ge 1$ or $\deg_A u''_2 \ge 1$. It also holds that $\deg_H u'_2 \ge 1$ or $\deg_H u''_2 \ge 1$ since $\max \{ \deg_H \phi_1, \deg_H \phi_2 \} = 2$. Therefore, since \tilde{u}'_2 and \tilde{u}''_2 are not constant, we can take polynomials v' and v'' satisfying the following properties by replacing u'_2 and u''_2 if necessary:

 $\begin{aligned} & - v'|u'_2 \text{ and } v''|u''_2, \\ & - \deg v' = 1 \text{ and } \deg v'' = 1, \\ & - \deg_A v' = 1 \text{ and } \deg_H v'' = 1. \end{aligned}$

We put $v' = e'_1 A + e'_2 H + e'_3 C + e'_4 Z$ and $v'' = e''_1 A + e''_2 H + e''_3 C + e''_4 Z$, where $e'_1 \neq 0$, $e''_2 \neq 0$, and $e'_1, \ldots, e'_4, e''_1, \ldots e''_4 \in \mathbb{Z}$. We now consider the following two cases:

1. Equations $v'(\alpha, 1, h, 1) = 0$ and $v''(\alpha, 1, h, 1) = 0$ have no common roots.

2. Equations $v'(\alpha, 1, h, 1) = 0$ and $v''(\alpha, 1, h, 1) = 0$ have a common root.

Case 1: Note that

$$v'(\alpha, 1, h, 1) = e'_1 \alpha + e'_2 h + e'_3 + e'_4, v''(\alpha, 1, h, 1) = e''_1 \alpha + e''_2 h + e''_3 + e''_4,$$

and $e'_1, e''_2 \neq 0$. Since there are no common roots of polynomials $v'(\alpha, 1, h, 1)$ and $v''(\alpha, 1, h, 1)$, it holds that $(e'_1 : e'_2) = (e''_1 : e''_2)$. Put $r = e'_2/e'_1 \neq 0$. From the equations (13), by substituting $\alpha = -rh$ into $\tilde{\phi}_1$ and $\tilde{\phi}_2$, they become polynomials of degree 2 or less. By substituting $\alpha = -rh$ into (12), we have

$$(-c_1)(3-4r)rh^3 + c_2(3-4r)h^2 + (-9c_1r - 3c_5'r + 2c_5')h + 9c_2.$$

Since this polynomial should be of degree 2 or less, it holds that r = 3/4 or $c_1 = 0$. By substituting $\alpha = -rh$ into (11), we have

$$(27c_1+3c_5')r^2h^4-27c_2rh^3+(c_1r^2+36c_5'-18c_5'r-48c_1r)h^2+(-r+48)c_2h-4c_5'.$$

Since this polynomial should also be of degree 2 or less, we have $c_2 = 0$ and $c'_5 = -9c_1$. Since $\tilde{\phi}_2(\alpha, h) \neq 0$, we have $c_1 \neq 0$ and r = 3/4. Next, we substitute $\alpha = -rh + r'$, where r' is a rational number such that

v'(-rh + r', 1, h, 1) = 0. By substituting $\alpha = -rh + r'$ into (13), these equations become $(\tilde{u}_2''(-rh + r', h))^2$ multiplied by a constant. We have

$$\tilde{\phi}_2(-rh+r',h) = -3c_1r'h^2 + (4r'^2 - 9/2)c_1h - 18c_1r'$$

by substituting $\alpha = -rh + r'$ into (12). As the degree of $\phi_2(-rh + r', h)$ must be even, we have $r' \neq 0$. Since the equation $\tilde{\phi}_2(-rh + r', h) = 0$ has only one root, it holds that $(4r'^2 - 9/2)^2 - 4(3r')(18r') = 0$. However, it is easy to check that the roots of this equation are not in \mathbb{Q} . This contradicts $r' \in \mathbb{Q}$.

Case 2: Denote a common root of $v'(\alpha, 1, h, 1)$ and $v''(\alpha, 1, h, 1)$ by (α_0, h_0) . Since

$$\psi_3 \cdot \varphi = \tilde{\phi}_1 - (-6h^3 + \alpha h^2 + 6h)\tilde{\phi}_2,$$

we have $\psi_3(\alpha_0, h_0)\varphi(\alpha_0, h_0) = 0$, where ψ_3 is the 3rd division polynomial of generalized Montgomery coordinates. From equations (12) and (10), it holds that

$$4\tilde{\phi}_2 - (3\alpha + 2h) \cdot \varphi = 3\alpha^2(c_1\alpha + c_2) + 36c_1\alpha + 36c_2 = 3(c_1\alpha + c_2)(\alpha^2 + 12).$$

Therefore, if $\varphi(\alpha_0, h_0) = 0$, we have $c_1\alpha_0 + c_2 = 0$ since $\alpha_0 \in \mathbb{Q}$. From the equation (10), it holds that $c'_5 = 0$. However, it is easy to see that if $c'_5 = 0$, then $\tilde{\phi}_1$ and $\tilde{\phi}_2$ can be divided by $c_1 \alpha + c_2$. This is a contradiction because $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 = 2$. Thus, we have $\varphi(\alpha_0, h_0) \neq 0$ and $\psi_3(\alpha_0, h_0) = 0$. Note that $h_0 \neq 0$ because $\psi_3(\alpha, 0) = -1 \neq 0$. We have $\tilde{\phi}_1(\alpha, h_0)$ and $\tilde{\phi}_2(\alpha, h_0)$ are divisible by $(\alpha - \alpha_0)^2$ from the equations (13). Therefore, it holds that $\psi_3(\alpha, h_0)$ can be divided by $(\alpha - \alpha_0)^2$ since $\varphi(\alpha_0, h_0) \neq 0$. However, because $h_0 \neq 0$, we have that $\psi_3(\alpha, h_0)$ is of degree 1. This is a contradiction.

Both cases lead to contradictions. Therefore, there is at least one seed polynomial of degree 3.

b) Three seed polynomials of degree 2:

We denote seed polynomials of degree 2 by u'_2 , u''_2 , and u'''_2 . We only need to consider the case that there are only two seed polynomials of degree 4, and there are no seed polynomials of degree 3. We denote these two polynomials of degree 4 by u'_4 and u''_4 . We want to show that at least two of these seed polynomials are obtained by multiplications. If 4 or more of these seed polynomials are obtained by squarings, then we have the following two cases:

- All seed polynomials of degree 2 and at least one seed polynomial of degree 4 are obtained by squarings.
- At least two seed polynomials of degree 2 and all seed polynomials of degree 4 are obtained by squarings.

Therefore, it is sufficient to prove that u_2'' and u_4'' should be obtained by multiplications when u'_2 , u''_2 , and u'_4 are obtained by squarings.

First, we prove the following claim:

Claim 5. Terms that do not appear in ϕ_1 and ϕ_2 (e.g., A^4 and C^4) also do not appear in u'_4 and u''_4 .

Proof of Claim 5. Suppose that there are terms that do not appear in ϕ_1 and ϕ_2 , but appear in u'_4 or u''_4 . Since we need to get rid of these terms from the results of the computation, the computational results are represented by $d_3(d_1u'_4 + d_2u''_4)$ and $d_4(d_1u'_4 + d_2u''_4)$ for some $d_1, \ldots, d_4 \in \mathbb{Z}$. This contradicts the fact that ϕ_1/ϕ_2 is not constant. We conclude that the terms that do not appear in ϕ_1 and ϕ_2 also do not appear in u'_4 and u''_4 . \square

Put $u'_4 = (d_1u'_2 + d_2u''_2 + d_3u'''_2)^2$, where $d_1, d_2, d_3 \in \mathbb{Z}$. There are no A^2 , AC, C^2 , H^2 , HZ, and Z^2 terms in $d_1u'_2 + d_2u''_2 + d_3u'''_2$ from Claim 5 and the fact that there are no A^4 , A^2C^2 , C^4 , H^4 , H^2Z^2 , and Z^4 terms in ϕ_1 and ϕ_2 . We define a (6×3) -matrix V as its *i*-th column is an alignment of coefficients of A^2 , AC, C^2 , H^2 , HZ, and Z^2 terms in $u_2^{(i)}$. From the above, the vector $V \cdot {}^t(d_1, d_2, d_3)$ is the zero vector, where t^* is a symbol for transpose. Therefore, it holds that rank $V \leq 2$. Since u'_2 and u''_2 are obtained by squarings, the matrix V is non-zero. Therefore, we have rank V = 1 or rank V = 2.

Case rank V = 1: Since rank V = 1, we have

$$u_{2}'(A, C, H, Z) = e_{7}(e_{5}(e_{1}A + e_{2}C) + e_{6}(e_{3}H + e_{4}Z))^{2},$$

$$u_{2}''(A, C, H, Z) = e_{8}(e_{5}(e_{1}A + e_{2}C) - e_{6}(e_{3}H + e_{4}Z))^{2},$$

for some $e_1, \ldots, e_8 \in \mathbb{Z}$. If $\deg_{A,C} u_2^{\prime\prime\prime} = 2$ or $\deg_{H,Z} u_2^{\prime\prime\prime} = 2$, then

$$u_{2}^{\prime\prime\prime}(A, C, H, Z) = (e_{5}^{\prime}(e_{1}A + e_{2}C) + e_{6}^{\prime}(e_{3}H + e_{4}Z))(e_{5}^{\prime\prime}(e_{1}A + e_{2}C) + e_{6}^{\prime\prime}(e_{3}H + e_{4}Z)) = e_{9}(e_{5}^{2}(e_{1}A + e_{2}C)^{2} + e_{6}^{2}(e_{3}H + e_{4}Z)^{2}) + e_{10}(e_{1}A + e_{2}C)(e_{3}H + e_{4}Z),$$

where $e'_5, e''_5, e'_6, e''_6, e_9, e_{10} \in \mathbb{Z}$, $e_{10} = e'_5 e''_6 + e''_5 e'_6$, $e'_5 e''_5 = e_9 e_5^2$, and $e'_6 e''_6 = e_9 e_6^2$. In this case, it holds that u'_4 and u''_4 can be divisible by $(e_1 A + e_2 C)(e_3 H + e_4 Z)$. This contradicts the degree of $\tilde{\phi}_1/\tilde{\phi}_2$ is 4. If $\deg_{A,C} u'''_2 = \deg_{H,Z} u'''_2 = 1$, then it holds that

$$u_2'''(A, C, H, Z) = (e_{11}A + e_{12}C)(e_{13}H + e_{14}Z),$$

where $e_{11}, \ldots, e_{14} \in \mathbb{Z}$. Therefore, we can compute seed polynomials of degree 4 by using $(e_1A + e_2C)(e_3H + e_4Z)$ and $(e_{11}A + e_{12}C)(e_{13}H + e_{14}Z)$. Hence, we can reduce this case to one that there are only two seed polynomials of degree 2. From the same discussion for the case of two seed polynomials of degree 2, there is at least one seed polynomial of degree 3. This is a contradiction.

Case rank V = 2: Note that $d_1u'_2 + d_2u''_2 + d_3u'''_2$ does not have terms of degree 2 in the variables of A, C or H, Z as mentioned before. Since rank V = 2, if it holds that $V \cdot {}^t(d'_1, d'_2, d'_3) = 0$, then the vector (d'_1, d'_2, d'_3) is in $\mathbb{Q}(d_1, d_2, d_3)$. Let

$$u_4'' = (d_1''u_2' + d_2''u_2'' + d_3''u_2''')(d_1'''u_2' + d_2'''u_2'' + d_3'''u_2''')$$

for $d_1'', d_2'', d_3'', d_1''', d_2'', d_3''' \in \mathbb{Z}$. Since $\gcd(u_4', u_4'') \in \mathbb{Z}$, we have (d_1'', d_2'', d_3'') is not in $\mathbb{Q}(d_1, d_2, d_3)$. Therefore, the polynomial $d_1''u_2' + d_2''u_2'' + d_3''u_2'''$ has terms of degree 2 in the variables of A, C or H, Z. Because u_4'' does not have $A^4, A^2C^2, C^4, H^4, H^2Z^2$, and Z^4 terms, the seed polynomial u_4'' should be obtained by a multiplication.

We now prove that $u_{2''}^{\prime\prime\prime}$ is obtained by a multiplication. Suppose that $u_{2''}^{\prime\prime\prime}$ is obtained by a squaring. Note that we need a multiplication of polynomials with terms of degree 2 in the variables of A, C or H, Z to compute $u_{4'}^{\prime\prime}$. From Claim 5, we can put

$$u_4''(A, C, H, Z) = (e_1A^2 + e_2AC + e_3C^2)(e_4H^2 + e_5HZ + e_6Z^2),$$

where $e_1, \ldots, e_6 \in \mathbb{Z}$. Let W_1 and W_2 be (3×3) -matrices satisfying $V = {}^t({}^tW_1 | {}^tW_2)$. There are vectors (d'_1, d'_2, d'_3) and (d''_1, d''_2, d''_3) such that

$$V \cdot {}^{t}(d'_{1}, d'_{2}, d'_{3}) = {}^{t}(e_{1}, e_{2}, e_{3}, 0, 0, 0), \quad V \cdot {}^{t}(d''_{1}, d''_{2}, d''_{3}) = {}^{t}(0, 0, 0, e_{4}, e_{5}, e_{6}).$$

Since rank V = 2, it holds that rank $W_1 = \operatorname{rank} W_2 = 1$. Therefore, polynomials u'_2 , u''_2 , and u'''_2 can be represented by

$$u_{2}'(A, C, H, Z) = (e_{11}(e_{7}A + e_{8}C) + e_{12}(e_{9}H + e_{10}Z))^{2},$$

$$u_{2}''(A, C, H, Z) = (e_{13}(e_{7}A + e_{8}C) + e_{14}(e_{9}H + e_{10}Z))^{2},$$

$$u_{2}'''(A, C, H, Z) = (e_{15}(e_{7}A + e_{8}C) + e_{16}(e_{9}H + e_{10}Z))^{2},$$

for some $e_7, \ldots, e_{16} \in \mathbb{Z}$. It is easy to check that u'_4 and u''_4 can be divided by $(e_7A + e_8C)(e_9H + e_{10}Z)$. This is a contradiction. Therefore, u''_2 is obtained by a multiplication.

Consequently, we proved u''_4 and u''_2 are obtained by multiplications. Therefore, the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more.

From the above discussions, we complete the proof of Lemma 18.

Lemma 19. Let $(\phi_1 : \phi_2)$ be a projective formula to compute image curves of 3-isogenies such that the degree of the formula is 4 (i.e., $\deg \phi_1 = \deg \phi_2 = 4$ and ϕ_1/ϕ_2 is irreducible over \mathbb{Z}). If $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 = 1$, the cost to compute this formula is $2\mathbf{M} + 3\mathbf{S}$ or more.

Proof. Let $\tilde{\phi}_1(\alpha, h)/\tilde{\phi}_2(\alpha, h)$ be an affine formula corresponding to $(\phi_1 : \phi_2)$. As we have already seen, there is a polynomial $\varphi(\alpha, h) \in \mathbb{Z}[\alpha, h]$ such that

$$\frac{\phi_1}{\tilde{\phi}_2} = -6h^3 + \alpha h^2 + 6h + (3h^4 + 4\alpha h^3 + 6h^2 - 1)\frac{\varphi}{\tilde{\phi}_2}$$

Since deg $\tilde{\phi}_1 \leq 4$ and deg_h $\tilde{\phi}_2 \leq 3$, polynomials φ and $\tilde{\phi}_2$ can be represented by

$$\phi_2(\alpha, h) = (3h + 4\alpha)h(c_1h + c_2) + c_4\alpha + c_5h + c_6, \varphi(\alpha, h) = (6h - \alpha)(c_1h + c_2) + c_3,$$

where $c_1, \ldots, c_6 \in \mathbb{Z}$. Since $\deg_{\alpha} \tilde{\phi}_1 \leq 1$ and $\deg_h \tilde{\phi}_1 \leq 3$, it holds that $c_4 = 0$ and $c_3 = 2c_5 - 18c_1$. Then, we have

$$\phi_1(\alpha, h) = (-54c_1 + 9c_5)\alpha h^3 + (18c_2 + c_6)\alpha h^2 + (54c_2 - 6c_6)h^3 + c_1\alpha h + (-114c_1 + 18c_5)h^2 + (-6c_2 + 6c_6)h + c_2\alpha + 18c_1 - 2c_5, \quad (14)$$
$$\tilde{\phi}_2(\alpha, h) = (3h + 4\alpha)h(c_1h + c_2) + c_5h + c_6. \quad (15)$$

From Lemma 13, we only need to consider the case that the highest degree of seed polynomials appearing in the computation is 4. From the proof of Lemma 12, there are two different seed polynomials of degree 2. Since there are at least two different seed polynomials of degree 4, if the number of seed polynomials of degree 2 is four or more, then the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more. Hence, we only need to consider the following cases:

a) There are two seed polynomials of degree 2.

b) There are three seed polynomials of degree 2.

a) Two seed polynomials of degree 2:

We denote seed polynomials of degree 2 by u'_2 and u''_2 . If there is a seed polynomial of degree 3 in the computation, the cost of the computation is $2{\bf M}+$ 3S or more as the diagram (9). Suppose that there is no seed polynomial of degree 3 in the computation. Put $\tilde{u}'_2(\alpha, h) = u'_2(\alpha, 1, h, 1)$ and $\tilde{u}''_2(\alpha, h) = u''_2(\alpha, 1, h, 1)$. Then, there are integers $d'_1, d'_2, d'_3, d''_1, d''_2, d''_3$ satisfying

$$\begin{split} \tilde{\phi}_1(\alpha,h) &= d_1' \tilde{u}_2'^2 + d_2' \tilde{u}_2' \tilde{u}_2'' + d_3' \tilde{u}_2''^2, \\ \tilde{\phi}_2(\alpha,h) &= d_1'' \tilde{u}_2'^2 + d_2'' \tilde{u}_2' \tilde{u}_2'' + d_3'' \tilde{u}_2''^2. \end{split}$$

If necessary, we replace u'_2 and u''_2 . We can assume that $\deg_{\alpha} \tilde{u}'_2 \ge 1$. Note that u'_2 is a seed polynomial. There are $r, r' \in \mathbb{Q}$ such that $\tilde{u}'_2(rh + r', h) = 0$. We have

$$\tilde{\phi}_1(rh+r',h) = d'_3 \cdot \tilde{u}''_2(rh+r',h)^2, \quad \tilde{\phi}_2(rh+r',h) = d''_3 \cdot \tilde{u}''_2(rh+r',h)^2.$$

From the equation (15), it holds that

$$\tilde{\phi}_2(rh+r',h) = (3+4r)c_1h^3 + (4c_1r'+3c_2+4c_2r)h^2 + (c_5+4c_2r')h + c_6.$$
(16)

From the equation (14), we have

$$\phi_1(rh + r', h) = (-54c_1 + 9c_5)rh^4 + ((-54c_1 + 9c_5)r' + (18c_2 + c_6)r + 54c_2 - 6c_6)h^3 + ((18c_2 + c_6)r' - 114c_1 + 18c_5 + c_1r)h^2 + (c_1r' - 6c_2 + 6c_6 + c_2r)h + c_2r' + 18c_1 - 2c_5.$$
(17)

We now have the following two cases:

Case 1: $\tilde{\phi}_2(rh + r', h) = 0.$ Case 2: $\tilde{\phi}_2(rh + r', h) \neq 0.$

Case 1: If $c_1 = 0$, then $c_6 = 0$, $c_5 + 4c_2r' = 0$, and $(3 + 4r)c_2 = 0$. Since at least one of c_1, c_2, c_5, c_6 is not zero, we have $c_6 = 0, c_2 \neq 0, r = -3/4$, and $c_5 + 4c_2r' = 0$. In this case, we have

$$\tilde{\phi}_1(rh+r',h) = -\frac{27}{4}c_5h^4 + \frac{-9c_5^2 + 162c_2^2}{4c_2}h^3 + \frac{27}{2}c_5h^2 - \frac{27}{4}c_2h - \frac{9}{4}c_5$$
$$= -\frac{9}{4c_2}(3c_2h+c_5)(c_5h^3 - 6c_2h^2 + c_2).$$

Since $\tilde{\phi}_1(rh+r',h) = d'_3 \cdot \tilde{u}''_2(rh+r',h)^2$, it holds that

$$c_5\left(\frac{-c_5}{3c_2}\right)^3 - 6c_2\left(\frac{-c_5}{3c_2}\right)^2 + c_2 = 0.$$

We have $27c_2^4 - 18c_2^2c_5^2 - c_5^4 = 0$. However, the equation $27x^4 - 18x^2 - 1 = 0$ has no root in \mathbb{Q} . This is a contradiction.

If $c_1 \neq 0$, then $c_6 = 0$, r = -3/4, r' = 0, and $c_5 = 0$. In this case, we have

$$\tilde{\phi}_1(rh+r',h) = \frac{81}{2}c_1h^4 + \frac{81}{2}c_2h^3 - \frac{459}{4}c_1h^2 - \frac{27}{4}c_2h + 18c_1$$
$$= \frac{9}{4}(6h^2 - 1)(3c_1h^2 + 3c_2h - 8c_1).$$

Since $\tilde{\phi}_1(rh+r',h) = d'_3 \cdot \tilde{u}''_2(rh+r',h)^2$, it holds

$$\frac{c_1}{2} + \frac{3c_2}{\sqrt{6}} - 8c_1 = 0.$$

Therefore, we have $c_1 = c_2 = 0$. However, this contradicts $c_1 \neq 0$.

Case 2: Since deg $(\tilde{\phi}_2(rh+r',h)) \leq 3$ and $\tilde{\phi}_2(rh+r',h) \neq 0$, it holds that deg $(\tilde{u}_2''(rh+r',h)) \leq 1$. Therefore, it holds that deg $(\tilde{u}_2''(rh+r'',h)) \leq 1$ for any $r'' \in \mathbb{Q}$ because \tilde{u}_2'' can be represented by

$$\tilde{u}_2''(\alpha,h) = w(\alpha,h) \cdot (\alpha - rh - r') + \tilde{u}_2''(rh + r',h),$$

where w is a polynomial of degree 1 or less in $\mathbb{Q}[\alpha, h]$, and we have

$$\tilde{u}_{2}''(rh+r'',h) = w(rh+r'',h) \cdot (r''-r') + \tilde{u}_{2}''(rh+r',h).$$

Therefore, from equations (16) and (17), it holds that

$$(3+4r)c_1 = 0, \quad (-54c_1+9c_5)r = 0, (-54c_1+9c_5)r'' + (18c_2+c_6)r + 54c_2 - 6c_6 = 0$$

for any $r'' \in \mathbb{Q}$. Then, we have

$$(3+4r)c_1 = 0$$
, $c_5 = 6c_1$, $(18c_2 + c_6)r + 54c_2 - 6c_6 = 0$.

Hence, there are the following cases:

Case (i):
$$r = -3/4$$
.

Case (ii): $c_1 = 0$ and $r \neq -3/4$.

Case (i): In this case, we have

$$-(18c_2+c_6)\frac{3}{4}+54c_2-6c_6=0.$$

Therefore, it holds that $c_6 = 6c_2$, and

$$\tilde{\phi}_2(rh+r',h) = 4c_1r'h^2 + (6c_1+4c_2r')h + 6c_2.$$

If $\tilde{\phi}_2(rh + r', h)$ is a constant, then we have $c_1 = r' = 0$ or $c_1 = c_2 = 0$. Since $c_1 = 0$ and $c_2 = 0$ leads to $c_5 = 0$ and $c_6 = 0$ respectively, we have $c_1 = r' = 0$. Thus, it holds that

$$\tilde{\phi}_1(rh+r',h) = (-6c_2 + 36c_2 - \frac{3}{4}c_2)h = \frac{117}{4}c_2h$$

from the equation (17). However, $\tilde{\phi}_1(rh + r', h)$ is a constant because $\tilde{u}_2''(rh + r', h)^2$ is a constant. This is a contradiction. Therefore, we have $\tilde{\phi}_2(rh + r', h)$ is not a constant.

Because deg $(\tilde{\phi}_2(rh+r',h)) \ge 1$ from the above, we have $c_1r' \ne 0$ and the equation $\tilde{\phi}_2(rh+r',h) = 0$ has only one root. Therefore,

$$(6c_1 + 4c_2r')^2 - 4 \cdot (4c_1r') \cdot (6c_2) = (6c_1 - 4c_2r')^2 = 0.$$

We have $3c_1 = 2c_2r'$, and the root of $\tilde{\phi}_2(rh + r', h) = 0$ is h = -3/2r'. From the equation (17),

$$\tilde{\phi}_1(rh+r',h) = \frac{117}{4}c_1h^2 + \frac{8r'^2 + 351}{8r'}c_1h + \frac{15}{2}c_1$$

Since h = -3/2r' is also a root of $\tilde{\phi}_1(rh + r', h) = 0$, we have

$$\frac{117}{4} \cdot \frac{9}{4r'^2}c_1 - \frac{8r'^2 + 351}{8r'} \cdot \frac{3}{2r'}c_1 + \frac{15}{2}c_1 = 0.$$

However, the left-hand side of the above equation equals $6c_1$. This is a contradiction.

Case (ii): In this case, we have $c_5 = 0$. Therefore,

$$\tilde{\phi}_2(rh+r',h) = (3+4r)c_2h^2 + 4c_2r'h + c_6,$$

$$\tilde{\phi}_1(rh+r',h) = (18c_2+c_6)r'h^2 + (-6c_2+6c_6+c_2r)h + c_2r'.$$
(18)

If $c_2 = 0$, then $\tilde{u}_2''(rh + r', h)$ is a constant. Therefore, the polynomial $\tilde{\phi}_1(rh + r', h)$ is also a constant, and we have $c_6 = 0$. This is a contradiction. Hence, we have $c_2 \neq 0$.

Since $c_2 \neq 0$ and $3 + 4r \neq 0$, it holds that $\tilde{\phi}_2(rh + r', h) = 0$ has only one root. Therefore,

$$(2c_2r')^2 - (3+4r)c_2 \cdot c_6 = 0.$$

From $c_2 \neq 0$, we have $c_6 = \frac{4r'^2}{3+4r}c_2$. It holds that

$$\tilde{\phi}_2(rh+r',h) = (3+4r)c_2\left(h+\frac{2r'}{3+4r}\right)^2.$$

Therefore, we have $\tilde{\phi}_1\left(-\frac{2r'}{3+4r}r+r',-\frac{2r'}{3+4r}\right)=0$. By substituting this and $c_6=\frac{4r'^2}{3+4r}c_2$ into the equation (18), we have

$$\left(18 + \frac{4r'^2}{3+4r}\right)r'\left(-\frac{2r'}{3+4r}\right)^2 + \left(r-6 + \frac{24r'^2}{3+4r}\right)\left(-\frac{2r'}{3+4r}\right) + r' = 0.$$

If r' = 0, then $c_6 = 0$ and $\tilde{\phi}_1(r'h+r,h) = (r-6)c_2h$. Therefore, we have r = 6 since deg $(\tilde{\phi}_1(r'h+r,h))$ is even. Then, it holds that $c_2 = 0$ from

 $(18c_2 + c_6)r + 54c_2 - 6c_6 = 0$. This is a contradiction. Therefore, it holds that $r' \neq 0$. From $r' \neq 0$, we have

$$\left(18 + \frac{4r'^2}{3+4r}\right)\frac{4r'^2}{(3+4r)^2} - \left(r-6 + \frac{24r'^2}{3+4r}\right)\left(\frac{2}{3+4r}\right) + 1 = 0.$$
(19)

Since $(18c_2 + c_6)r + 54c_2 - 6c_6 = 0$ and $c_6 = \frac{4r'^2}{3+4r}c_2$, it holds that

$$4r'^2 = (3+4r)\frac{18r+54}{6-r}.$$

Substituting this into the equation (19), we have

$$\frac{(2r+15)(r^2+96r+360)}{(6-r)^2(3+4r)} = 0$$

Since $r \in \mathbb{Q}$, we have $r = -\frac{15}{2}$. Therefore, it holds that

$$4r^{\prime 2} = \left(3 - 4 \cdot \frac{15}{2}\right) \frac{-18 \cdot \frac{15}{2} + 54}{6 + \frac{15}{2}} = 162$$

This contradicts $r \in \mathbb{Q}$.

Therefore, in both Case (i) and Case (ii), there are contradictions.

Consequently, in all cases, there are contradictions. Hence, there is a seed polynomial of degree 3 in the computation, and the cost of this computation is $2\mathbf{M} + 3\mathbf{S}$ or more.

b) Three seed polynomials of degree 2:

We can suppose that there are only two seed polynomials of degree 4. We denote these two polynomials by u'_4 and u''_4 . We now prove that these seed polynomials are obtained by multiplications. For the same reason as Claim 5 in the proof of Lemma 18, these polynomials do not have terms of degree other than 1 in the variables A and C. Thus, it holds that $\deg_{A,C} u'_4 = \deg_{A,C} u''_4 = 1$. Therefore, u'_4 and u''_4 are obtained by multiplications, and the cost of this computation is $2\mathbf{M} + 3\mathbf{S}$ or more.

From the above discussions, we conclude that the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more. This completes the proof of Lemma 19.

Lemma 20. Let $(\phi_1 : \phi_2)$ be a projective formula to compute image curves of 3-isogenies such that the degree of the formula is 4 (i.e., $\deg \phi_1 = \deg \phi_2 = 4$ and ϕ_1/ϕ_2 is irreducible over \mathbb{Z}). If $\deg_{A,C} \phi_1 = \deg_{A,C} \phi_2 = 0$, it holds that

$$(\phi_1:\phi_2) = (-27H^4 + 18H^2Z^2 + Z^4: 4HZ^3).$$

Moreover, the least cost to compute this formula is $2\mathbf{M} + 3\mathbf{S}$.

Proof. Let $\tilde{\phi}_1(\alpha, h)/\tilde{\phi}_2(\alpha, h)$ be an affine formula corresponding to $(\phi_1 : \phi_2)$. As we have already seen, there is a polynomial $\varphi(\alpha, h) \in \mathbb{Z}[\alpha, h]$ such that

$$\frac{\bar{\phi}_1}{\bar{\phi}_2} = -6h^3 + \alpha h^2 + 6h + (3h^4 + 4\alpha h^3 + 6h^2 - 1)\frac{\varphi}{\bar{\phi}_2}.$$

Since deg $\tilde{\phi}_1 \leq 4$, if deg $\tilde{\phi}_2 \geq 2$, then the highest degree terms of $\tilde{\phi}_2$ can be divided by $h(3h + 4\alpha)$. As deg_{α} $\tilde{\phi}_2 = 0$, we have deg $\tilde{\phi}_2 \leq 1$. It is clear that deg $\varphi = 0$. We let $\varphi(\alpha, h) = c_1$, and $\tilde{\phi}_2(\alpha, h) = c_2h + c_3$, where $c_1, c_2, c_3 \in \mathbb{Z}$. Since deg_{α} $\tilde{\phi}_1 = 0$, it is easy to check that $c_2 = -4c_1$ and $c_3 = 0$. Therefore,

$$\frac{\tilde{\phi}_1}{\tilde{\phi}_2} = \frac{-27h^4 + 18h^2 + 1}{4h},$$

and it holds that

$$(\phi_1:\phi_2) = (-27H^4 + 18H^2Z^2 + Z^4: 4HZ^3).$$

Now, we prove the cost of this formula is $2\mathbf{M} + 3\mathbf{S}$ or more. By substituting A = 0 and C = 0, we can assume all seed polynomials appearing in the computation are polynomials in $\mathbb{Z}[H, Z]$. From Lemma 13, we only need to consider the case that the highest degree of seed polynomials appearing in the computation is 4. From the proof of Lemma 12, there are two different seed polynomials of degree 2. Since there are at least two different seed polynomials of degree 4, we only need to consider the following cases:

- a) There are two seed polynomials of degree 2.
- b) There are three seed polynomials of degree 2.

a) Two seed polynomials of degree 2:

We denote two seed polynomials of degree 2 by u'_2 and u''_2 . From the diagram (9), if there is a seed polynomial of degree 3 in the computation, then the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more. Suppose that there is no seed polynomial of degree 3 in the computation.

In this case, polynomials ϕ_1 and ϕ_2 can be represented by linear combinations of $u_2'^2$, $u_2'u_2''$, and $u_2''^2$. We put

$$u'_{2} = e_{1}H^{2} + e_{2}HZ + e_{3}Z^{2}, \quad u''_{2} = e'_{1}H^{2} + e'_{2}HZ + e'_{3}Z^{2},$$

where $e_1, e_2, e_3, e'_1, e'_2, e'_3 \in \mathbb{Z}$. Then, vectors ${}^t(-27, 0, 18, 0, 1)$ and ${}^t(0, 0, 0, 4, 0)$ are linear combinations of the following vectors:

$$v_{1} := \begin{pmatrix} e_{1}^{2} \\ 2e_{1}e_{2} \\ 2e_{1}e_{3} + e_{2}^{2} \\ 2e_{2}e_{3} \\ e_{3}^{2} \end{pmatrix}, \quad v_{2} := \begin{pmatrix} e_{1}e_{1}' \\ e_{1}e_{2}' + e_{2}e_{1}' \\ e_{1}e_{3}' + e_{2}e_{2}' + e_{3}e_{1}' \\ e_{2}e_{3}' + e_{3}e_{2}' \\ e_{3}e_{3}' \end{pmatrix}, \quad v_{3} := \begin{pmatrix} e_{1}'^{2} \\ 2e_{1}'e_{2}' \\ 2e_{1}'e_{3}' + e_{2}'^{2} \\ 2e_{1}'e_{3}' + e_{2}'^{2} \\ 2e_{2}'e_{3}' \\ e_{3}'^{2} \end{pmatrix}.$$

Focusing on ${}^{t}(-27, 0, 18, 0, 1)$, we have $(e_1, e'_1) \neq (0, 0)$ and $(e_3, e'_3) \neq (0, 0)$. Moreover, focusing on ${}^{t}(0, 0, 0, 4, 0)$, we have $(e_2, e'_2) \neq (0, 0)$. Therefore, it is easy to see that at least one of the second components of v_1, v_2, v_3 is not zero. We let *i* be an integer such that v_i is a vector whose second component is not zero. Then, $\{v_i, {}^{t}(-27, 0, 18, 0, 1), {}^{t}(0, 0, 0, 4, 0)\}$ is a basis of $\langle v_1, v_2, v_2 \rangle$. Hence, if the second component of $v \in \langle v_1, v_2, v_3 \rangle$ is zero, then *v* is a linear combination of ${}^{t}(-27, 0, 18, 0, 1)$ and ${}^{t}(0, 0, 0, 4, 0)$. By computing $(e_1e'_2 + e_2e'_1)v_1 - (2e_1e_2)v_2$, we have

$$(e_1e'_2 + e_2e'_1)v_1 - (2e_1e_2)v_2 = \begin{pmatrix} e_1^2(e_1e'_2 + e_2e'_1) - (2e_1e_2)(e_1e'_1) \\ 0 \\ * \\ e_3^2(e_1e'_2 + e_2e'_1) - e_3e'_3(2e_1e_2) \end{pmatrix}.$$

Since this vector is a linear combination of ${}^{t}(-27, 0, 18, 0, 1)$ and ${}^{t}(0, 0, 0, 4, 0)$, we have

$$e_1^2(e_1e_2' + e_2e_1') - (2e_1e_2)(e_1e_1') = -27(e_3^2(e_1e_2' + e_2e_1') - e_3e_3'(2e_1e_2)).$$
(20)

By considering $(e_1e'_2 + e_2e'_1)v_3 - (2e'_1e'_2)v_2$ and $(e'_1e'_2)v_1 - (e_1e_2)v_3$, we also have

$$e_1^{\prime 2}(e_1e_2^{\prime} + e_2e_1^{\prime}) - (2e_1^{\prime}e_2^{\prime})(e_1e_1^{\prime}) = -27(e_3^{\prime 2}(e_1e_2^{\prime} + e_2e_1^{\prime}) - e_3e_3^{\prime}(2e_1^{\prime}e_2^{\prime})), \quad (21)$$

$$e_1^2(e_1'e_2') - e_1'^2(e_1e_2) = -27(e_3^2(e_1'e_2') - e_3'^2(e_1e_2)).$$
(22)

We now prove that $e_1, e_2, e_3, e'_1, e'_2, e'_3 \in \mathbb{Z} \setminus \{0\}$. Note that $(e_j, e'_j) \neq (0, 0)$ for all j = 1, 2, 3, and $(e_1, e_2, e_3) \neq (0, 0, 0)$, $(e'_1, e'_2, e'_3) \neq (0, 0, 0)$. Suppose that at least one of $e_1, e_2, e_3, e'_1, e'_2, e'_3$ is zero. From symmetry of e_1, e_2, e_3 and e'_1, e'_2, e'_3 , we only need to consider the cases of $e_1 = 0$, $e_2 = 0$, and $e_3 = 0$.

- **Case** $e_1 = 0$: Note that $e'_1 \neq 0$. Substituting $e_1 = 0$ into (20) and (22), we have $0 = e_3^2 e_2$ and $0 = e_3^2 e'_2$. Since $(e_2, e'_2) \neq (0, 0)$, it holds that $e_3 = 0$. Substituting $e_1 = e_3 = 0$ into (21), it holds that $(e'_1{}^2 + 27e'_3{}^2)e_2 = 0$. This contradicts $e'_1 \neq 0$, $e'_3 \neq 0$, and $e_2 \neq 0$.
- **Case** $e_2 = 0$: We can suppose $e_1 \neq 0$ from the previous case. Substituting $e_2 = 0$ into (20), we have $(e_1^2 + 27e_3^2)e_1 = 0$. Therefore, it holds that $e_1 = 0$. This is a contradiction.
- **Case** $e_3 = 0$: We can suppose $e_1 \neq 0$ and $e_2 \neq 0$. Substituting $e_3 = 0$ into (20), we have $e_1e'_2 = e_2e'_1$. Substituting $e_3 = 0$ and $e_1e'_2 = e_2e'_1$ into (20), we have $e'_3 = 0$. This is a contradiction.
- In all cases, there are contradictions. Therefore, $e_1, e_2, e_3, e'_1, e'_2, e'_3$ are not zeros. By calculating $(20) \times e'_1^2 + (21) \times e_1^2$, we have

$$0 = (e_3^2 e_1'^2 + e_1^2 e_3'^2)(e_1 e_2' + e_2 e_1') - 2e_1 e_3 e_1' e_3' (e_1 e_2' + e_2 e_1')$$

= $(e_1 e_3' - e_3 e_1')^2 (e_1 e_2' + e_2 e_1').$

Therefore, $e_1e'_3 = e_3e'_1$ or $e_1e'_2 + e_2e'_1 = 0$.

Case $e_1e'_2 + e_2e'_1 = 0$: From the equation (21), we have

$$(e_1'e_2')(e_1e_1') = -27(e_1'e_2')(e_3e_3')$$

Since $e'_1e'_2 \neq 0$, it holds that $e_1e'_1 = -27e_3e'_3$. By substituting $e_2e'_1 = -e_1e'_2$ and $e'_3 = (e_1e'_1)/(-27e_3)$ into the equation (22), we have

$$0 = e_1^2(e_1'e_2') - e_1'e_1(-e_1e_2') + 27e_3^2(e_1'e_2') - 27\left(\frac{e_1e_1'}{-27e_3}\right)^2(e_1e_2)$$

= $(2e_1^2 + 27e_3^2)(e_1'e_2') - \frac{e_1^3e_1'(-e_1e_2')}{27e_3^2}$
= $\frac{1}{27e_3^2}(54e_1^2e_3^2 + 27^2e_3^4 + e_1^4)(e_1'e_2').$

Since $54e_1^2e_3^2 + 27^2e_3^4 + e_1^4 \neq 0$ and $e_1'e_2' \neq 0$, this is a contradiction. Case $e_1e_3' = e_3e_1'$: From the equation (20), we have

$$e_1^2(e_1e_2' - e_2e_1') = -27e_3^2(e_1e_2' - e_2e_1').$$

Since $e_1^2 + 27e_3^2 \neq 0$, we have $e_1e_2' = e_2e_1'$. By substituting $e_2' = (e_2e_1')/e_1$ and $e_3' = (e_3e_1')/e_1$ into v_2 and v_3 , we have $v_2 = (e_1'/e_1)v_1$ and $v_3 = (e_1'^2/e_1^2)v_1$. This is a contradiction.

Hence, in each case, there are contradictions. We conclude that there is a seed polynomial of degree 3 in the computation, and the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more.

b) Three seed polynomials of degree 2:

We denote three seed polynomials of degree 2 by u'_2 , u''_2 , and u'''_2 . In this case, we can suppose that there are only two seed polynomials of degree 4. We denote these seed polynomials of degree 4 by u'_4 and u''_4 .

We now show that u'_4 and u''_4 are obtained by multiplications. Suppose that u'_4 is obtained by a squaring. Since there are no H^3Z terms in ϕ_1 and ϕ_2 , there are no H^3Z terms in u'_4 and u''_4 . Therefore, we can represent u'_4 by $u'_4 = (e_1H^2 + e_2Z^2)^2$ or $u'_4 = (e_1HZ + e_2Z^2)^2$, where $e_1, e_2 \in \mathbb{Z}$.

Case $u'_4 = (e_1H^2 + e_2Z^2)^2$: The seed polynomial u''_4 has the HZ^3 term since ϕ_2 has the HZ^3 term and u'_4 does not. Let $\phi_1 = d'_1u'_4 + d''_1u''_4$, where d'_1, d''_1 are integers. As ϕ_1 has no HZ^3 terms, we have $d''_1 = 0$. However, there are no integers d'_1, e_1, e_2 satisfying $\phi_1 = d'_1(e_1H^2 + e_2Z^2)^2$. This is a contradiction. **Case** $u'_4 = (e_1HZ + e_2Z^2)^2$: The seed polynomial u''_4 has the H^4 term since ϕ_1 has the U^4_4 term and u'_4 does not. Let $\phi_1 = d'_1u'_4 + d''_1u''_4$.

Case $u'_4 = (e_1HZ + e_2Z^2)^2$: The seed polynomial u''_4 has the H^4 term since ϕ_1 has the H^4 term and u'_4 does not. Let $\phi_2 = d'_2u'_4 + d''_2u''_4$, where $d'_2, d''_2 \in \mathbb{Z}$. As ϕ_2 has no H^4 terms, we have $d''_2 = 0$. However, there are no integers d'_2, e_1, e_2 satisfying $\phi_2 = d'_2(e_1HZ + e_2Z^2)^2$. This is a contradiction.

From the above discussions, it holds that u'_4 and u''_4 are obtained by multiplications, and the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more.

Consequently, the cost of the computation is $2\mathbf{M} + 3\mathbf{S}$ or more.

From [CH17, Appendix A] or the diagram (4), we have already known that this formula can be computed with the costs of $2\mathbf{M} + 3\mathbf{S}$. This completes the proof of Lemma 20.

5 Conclusion

In this paper, we analyzed the general formula to compute image curves of 3isogenies in the framework of generalized Montgomery coordinates. The lower bound of the costs of the formulas is $1\mathbf{M} + 1\mathbf{S}$ as an affine formula whose output is also affine, $2\mathbf{S}$ as an affine formula whose output is projective, and $2\mathbf{M} + 3\mathbf{S}$ as a projective formula under some heuristics. The formula

$$-6h^3 + \alpha h^2 + 6h^3$$

is one of the most efficient formulas as an affine formula whose output is also in affine coordinates, the formula

$$(-27h^4 + 18h^2 + 1:4h)$$

is one of the most efficient affine formulas, and the formula

$$(-27H^4 + 18H^2Z^2 + Z^4 : 4HZ^3)$$

is one of the most efficient projective formulas.

5.1 Future works

One of the most important future works of this study is to analyze formulas to compute image curves of high-degree isogenies. For recent isogeny-based schemes $(e.g., \text{CSIDH} [\text{CLM}^+18], \text{SQISign} [\text{DFKL}^+20])$ need computation of high-degree isogenies. Therefore, we should extend this result to isogenies of degree more than 3. Moreover, this extension is also an interesting problem for mathematics.

Another important direction is to make the analysis more precise. In this paper, we introduced some assumptions to make the analysis simplify. There is a possibility that these assumptions hide truly efficient formulas. Moreover, in practice, we often compute image curves and image points under isogenies (formula (1)) at the same time. This means some computation can be shared in the computation of these formulas. Therefore, we may be able to compute more efficiently by this sharing.

Acknowledgements.

This work was supported by JSPS KAKENHI Grant Number JP21J10711, JP21K17739, EPSRC through grant EP/V011324/1, and JST CREST Grant Number JPMJCR2113, Japan.

References

- CLM⁺18. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In Advances in Cryptology – ASIACRYPT 2018, pages 395–427. Springer, 2018.
- CH17. Craig Costello and Huseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In Advances in Cryptology – ASI-ACRYPT 2017, pages 303–329. Springer, 2017.
- CLN16. Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. In Annual International Cryptology Conference, pages 572–601. Springer, 2016.
- DFKL⁺20. Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. In Advances in Cryptology – ASIACRYPT 2020, pages 64–93. Springer, 2020.
- DKW20. Robert Dryło, Tomasz Kijko, and Michał Wroński. Efficient Montgomerylike formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptography. Cryptology ePrint Archive, Report 2020/526, 2020. https://ia.cr/2020/526.
- HZHL20. Yan Huang, Fangguo Zhang, Zhi Hu, and Zhijie Liu. Optimized arithmetic operations for isogeny-based cryptography on Huff curves. In *Information* Security and Privacy – ACISP 2020, pages 23–40. Springer, 2020.
- MR18. Michael Meyer and Steffen Reith. A faster way to the CSIDH. In Progress in Cryptology – INDOCRYPT 2018, pages 137–152. Springer, 2018.
- MOAT22. Tomoki Moriya, Hiroshi Onuki, Yusuke Aikawa, and Tsuyoshi Takagi. The generalized Montgomery coordinate: A new computational tool for Isogeny-based cryptography. *Mathematical Cryptology*, 2(1):36–59, 2022.
- Ren18. Joost Renes. Computing isogenies between Montgomery curves using the action of (0, 0). In Post-Quantum Cryptography – PQCrypto 2018, pages 229–247. Springer, 2018.
- Sil09. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.
- Vél71. Jacques Vélu. Isogénies entre courbes elliptiques. CR Acad. Sci. Paris Sér. A, 273(5):238–241, 1971.