Efficient Arithmetic on Hessian Curves

Reza R. Farashahi[1,2] and Marc Joye[3]

[1] Macquarie University, Department of Computing
Sydney, NSW 2109, Australia
reza@science.mq.edu.au
[2] Isfahan University of Technology, Department of Mathematical Sciences
P.O. Box 85145 Isfahan, Iran
[3] Technicolor, Security Competence Center
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
marc.joye@technicolor.com – http://www.thlab.net/~joyem/

Abstract. This paper considers a generalized form for Hessian curves. The family of generalized Hessian curves covers more isomorphism classes of elliptic curves. Over a finite filed $\mathbb{F}_q$, it is shown to be equivalent to the family of elliptic curves with a torsion subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$. This paper provides efficient unified addition formulas for generalized Hessian curves. The formulas even feature completeness for suitably chosen parameters.
This paper also presents extremely fast addition formulas for generalized binary Hessian curves. The fastest projective addition formulas require $9\mathbf{M} + 3\mathbf{S}$, where $\mathbf{M}$ is the cost of a field multiplication and $\mathbf{S}$ is the cost of a field squaring. Moreover, very fast differential addition and doubling formulas are provided that need only $5\mathbf{M} + 4\mathbf{S}$ when the curve is chosen with small curve parameters.

Keywords: Elliptic curves, Hessian curves, cryptography.

1 Introduction

An elliptic curve E over a field $\mathbb{F}$ can be given by the *Weierstraß equation*

$$E: \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6\,,$$

where the coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. Koblitz [26] and Miller [30] were the first to show that the group of rational points on an elliptic curve E over a finite field $\mathbb{F}_q$ can be used for the discrete logarithm problem in a public-key cryptosystem.

There are many other ways to represent elliptic curves such as Legendre equation, cubic equations, quartic equations and intersection of two quadratic surfaces [2, 32, 35]. Several forms of elliptic curves over finite fields with several coordinate systems have been studied to improve the efficiency and the speed of the arithmetic on the group law (mainly addition and doubling formulas) [2, 4].

Some *unified* addition formulas that also work for the point doubling have been presented for several forms of elliptic curves, see e.g. [23, 27, 8, 11, 10, 5].

Overviews can be found in [2, 9]. Moreover, *complete* addition formulas that work for all pairs of inputs have been presented for Edwards curves over odd characteristic fields [5], and for binary Edwards curves [6].

A Hessian curve over a field $\mathbb{F}$ is defined by a symmetric cubic equation

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

where $d \in \mathbb{F}$ and $d^3 \neq 27$. The use of Hessian curves in cryptography has been studied in [13, 23, 33, 21, 22]. The Hessian addition formulas, the so-called Sylvester formulas, can also be used for point doubling after a permutation of input coordinates, providing a weak form of unification. Moreover, the same formulas can be used to double, add, and subtract points, which makes Hessian curves interesting against side-channel attacks [23].

In this paper, we consider the family of curves, referred to as *generalized Hessian curves*, over a field $\mathbb{F}$ defined by the equation

$$X^3 + Y^3 + cZ^3 = dXYZ\,,$$

where $c, d \in \mathbb{F}$, $c \neq 0$ and $d^3 \neq 27c$. Clearly, this family covers more isomorphism classes of elliptic curves than Hessian curves. Notice that the Sylvester addition formulas work for the family of *generalized Hessian*. But these formulas are not unified. From the Sylvester formulas and after suitable transformation of inputs coordinates, we present fast and efficient *unified* addition formulas for generalized Hessian curves.

Nevertheless, the unified formulas for Hessian curves are not complete. In other words, there are some exceptional cases where the formulas fail to give the output. We study the exceptional cases of the addition formulas for generalized Hessian curves. We observe that the unified formulas are *complete* for many generalized Hessian curves, i.e., the addition formulas work for all pairs of inputs. In particular, the group of $\mathbb{F}$-rational points on a generalized Hessian curve has *complete* addition formulas if and only if c is not a cube in $\mathbb{F}$. Also, the unified formulas are valid for all input points in rational subgroups $\mathcal{H}$ of generalized Hessian curves over finite fields $\mathbb{F}_q$ whenever $\gcd(\#\mathcal{H}, 3) = 1$.

For generalized binary Hessian curves, the *unified* addition formulas are the fastest known addition formulas on binary elliptic curves; for example $9\mathbf{M} + 3\mathbf{S}$ for extended projective addition, $8\mathbf{M} + 3\mathbf{S}$ for extended mixed affine-projective addition, and $5\mathbf{M} + 4\mathbf{S}$ for mixed addition and doubling, when curves are chosen with small parameters. As usual, we use $\mathbf{M}$ to denote a field multiplication and $\mathbf{S}$ to denote a field squaring. Furthermore, the addition formulas are complete for generalized Hessian curves over $\mathbb{F}_{2^n}$ when c is not a cube in $\mathbb{F}_{2^n}$. The mixed differential addition and doubling formulas are also complete.

Note. In [7], Bernstein, Kohel, and Lange define the *twisted* Hessian form. The twisted form is similar to the above form up to the order of the coordinates. Both forms present advantages. The neutral element on the twisted form is a finite point. In affine coordinates, the generalized form is fully symmetric and features a simpler inverse. See also [12, Exerc. 6.2].

2 Generalized Hessian curves

A *Hessian curve* over a field $\mathbb{F}$ is given by the cubic equation

$$\mathrm{H}_d: \ x^3 + y^3 + 1 = dxy\,,$$

for some $d \in \mathbb{F}$ with $d^3 \neq 27$ [19]. This section considers the family of *generalized* Hessian curves which cover more isomorphism classes of elliptic curves than Hessian curves. As will be shown, this family provides efficient *unified* addition formulas. Moreover, the unified formulas are *complete* for some generalized Hessian curves, i.e., the addition formulas work for all pairs of inputs.

2.1 Definition

Definition 1. *Let c, d be elements of $\mathbb{F}$ such that $c \neq 0$ and $d^3 \neq 27c$. The generalized Hessian curve $\mathrm{H}_{c,d}$ over $\mathbb{F}$ is defined by the equation*

$$\mathrm{H}_{c,d} \ : \ x^3 + y^3 + c = dxy \ .$$

Clearly, a Hessian curve H_d is a *generalized Hessian* curve $\mathrm{H}_{c,d}$ with $c = 1$. Moreover, the *generalized Hessian* curve $\mathrm{H}_{c,d}$ over $\mathbb{F}$, via the map $(x, y) \mapsto (\widetilde{x}, \widetilde{y})$ defined by

$$\widetilde{x} = x/\zeta \quad \text{and} \quad \widetilde{y} = y/\zeta \tag{1}$$

with $\zeta^3 = c$, is isomorphic over $\overline{\mathbb{F}}$ to the Hessian curve $\mathrm{H}_{\frac{d}{\zeta}} \ : \ \widetilde{x}^3 + \widetilde{y}^3 + 1 = \frac{d}{\zeta}\widetilde{x}\widetilde{y}$. Therefore, for the j-invariant of $\mathrm{H}_{c,d}$, we have

$$j(\mathrm{H}_{c,d}) = j(\mathrm{H}_{\frac{d}{\zeta}}) = \frac{1}{c}\left(\frac{d(d^3 + 6^3 c)}{d^3 - 3^3 c}\right)^3 \ . \tag{2}$$

We see that the curve $\mathrm{H}_{c,d}$ over $\mathbb{F}$ is isomorphic to the curve $\mathrm{H}_{\frac{d}{\zeta}}$ over $\mathbb{F}$ if $\zeta \in \mathbb{F}$. In other words, a generalized Hessian curve over $\mathbb{F}$ is isomorphic over $\mathbb{F}$ to a Hessian curve if and only if c is a cube in $\mathbb{F}$.

It is easy to adapt the addition and doubling formulas for generalized Hessian curves (see e.g. [12, Formulary], a.k.a. Sylvester formulas). The sum of two (different) points (x_1, y_1), (x_2, y_2) on $\mathrm{H}_{c,d}$ is the point (x_3, y_3) given by

$$x_3 = \frac{{y_1}^2 x_2 - {y_2}^2 x_1}{x_2 y_2 - x_1 y_1} \quad \text{and} \quad y_3 = \frac{{x_1}^2 y_2 - {x_2}^2 y_1}{x_2 y_2 - x_1 y_1} \ . \tag{3}$$

The doubling of the point (x_1, y_1) on $\mathrm{H}_{c,d}$ is the point (x_3, y_3) given by

$$x_3 = \frac{y_1(c - {x_1}^3)}{{x_1}^3 - {y_1}^3} \quad \text{and} \quad y_3 = \frac{x_1(c - {y_1}^3)}{{x_1}^3 - {y_1}^3} \ . \tag{4}$$

Furthermore, the inverse of the point (x_1, y_1) on $\mathrm{H}_{c,d}$ is the point (y_1, x_1).

The projective closure of the curve $\mathrm{H}_{c,d}$ is

$$\mathbf{H}_{c,d}: \ X^3 + Y^3 + cZ^3 = dXYZ \ .$$

It has the points $(1 : -\omega : 0)$ with $\omega^3 = 1$ at infinity. The neutral element of the group of $\mathbb{F}$-rational points of $\mathbf{H}_{c,d}$ is the point at infinity $(1 : -1 : 0)$ that we denote by $\mathcal{O}$. For the point $P = (X_1 : Y_1 : Z_1)$ on $\mathbf{H}_{c,d}$, we have $-P = (Y_1 : X_1 : Z_1)$.

Point addition. Using the addition formulas (3), whenever defined, the sum of the points $(X_1 : Y_1 : Z_1)$, $(X_2 : Y_2 : Z_2)$ on $\mathbf{H}_{c,d}$ is the point $(X_3 : Y_3 : Z_3)$ with

$$X_3 = X_2Z_2{Y_1}^2 - X_1Z_1{Y_2}^2, \quad Y_3 = Y_2Z_2{X_1}^2 - Y_1Z_1{X_2}^2,$$
$$Z_3 = X_2Y_2{Z_1}^2 - X_1Y_1{Z_2}^2 \ . \quad (5)$$

The cost of point addition algorithms in [13, 23, 33] is $12\mathbf{M}$. Moreover, these addition formulas can be performed in a parallel way, see [33]. In particular, one can perform the addition formulas (5) in a parallel environment using $3, 4$ or 6 processors with the cost of $4\mathbf{M}$, $3\mathbf{M}$ or $2\mathbf{M}$, respectively. To gain speedup, one can use the extended coordinates $(X : Y : Z : X^2 : Y^2 : Z^2 : 2XY : 2XZ : 2YZ)$. The addition algorithm in [22] uses this modified system of coordinates for the Hessian curves over the field $\mathbb{F}$ of characteristic $p > 3$. This algorithm requires $6\mathbf{M} + 6\mathbf{S}$.

Point doubling. The doubling of the point $(X_1 : Y_1 : Z_1)$ on $\mathbf{H}_{c,d}$ is the point $(X_3 : Y_3 : Z_3)$ given by

$$X_3 = Y_1(c{Z_1}^3 - {X_1}^3), \quad Y_3 = X_1({Y_1}^3 - c{Z_1}^3), \quad Z_3 = Z_1({X_1}^3 - {Y_1}^3) \ . \quad (6)$$

From the doubling algorithm in [13], we have the following algorithm that needs $6\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$, where $\mathbf{D}$ is the cost of a multiplication by the constant c:

$$A = {X_1}^2, \ B = {Y_1}^2, \ C = {Z_1}^2, \ D = X_1A, \ E = Y_1B, \ F = cZ_1C,$$
$$X_3 = Y_1(F - D), \quad Y_3 = X_1(E - F), \quad Z_3 = Z_1(D - E) \ . \quad (7)$$

Moreover, the cost of the following doubling algorithm for curves $\mathbf{H}_{c,d}$ over a field $\mathbb{F}$ of characteristic $p \neq 2$ is $7\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$:

$$A = X_1Y_1, \ B = (X_1 + Y_1)^2 - 2A, \ C = (X_1 + Y_1)(B - A),$$
$$D = (X_1 - Y_1)(B + A), \ E = 3C - 2dAZ_1,$$
$$X_3 = Y_1(E + D), \quad Y_3 = X_1(D - E), \quad Z_3 = -2Z_1D \ . \quad (8)$$

Also, one can perform the doubling formulas (6) with a cost of $3\mathbf{M} + 3\mathbf{C} + 1\mathbf{D}$, where $\mathbf{C}$ denotes a field cubing. Furthermore, for Hessian curves $\mathbf{H}_{1,d}$ over the field $\mathbb{F}$ of characteristic $p \neq 2$, the doubling algorithms in [21, 22] use the extended coordinates which require $3\mathbf{M} + 6\mathbf{S}$.

2.2 Universality of the model

We study the correspondence between generalized Hessian curves and elliptic curves having a torsion subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$. In particular, we show that every elliptic curve over a finite field with a torsion subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$ has an isomorphic generalized Hessian model.

Theorem 1. *Let E be an elliptic curve over a field $\mathbb{F}$. If the group $E(\mathbb{F})$ has a point of order 3 then E is isomorphic over $\overline{\mathbb{F}}$ to a generalized Hessian curve. Moreover, if $\mathbb{F}$ has an element ω with $\omega^2+\omega+1=0$, then the group $E(\mathbb{F})$ has a point of order 3 if and only if E is isomorphic over $\mathbb{F}$ to a generalized Hessian curve.*

Proof. We note that the elliptic curve E over $\mathbb{F}$ has a point of order 3 if and only if it has a Weierstraß model $\mathbf{E}_{a_1,a_3} : y^2z + a_1xyz + a_3yz^2 = x^3$ (see e.g. [25]). Let $\omega \in \overline{\mathbb{F}}$ with $\omega^2+\omega+1=0$. Let p be the characteristic of $\mathbb{F}$.

1. If $p \neq 3$, the elliptic curve $\mathbf{E}_{a_1,a_3}$ via the map $(x,y,z) \mapsto (X,Y,Z)$ given by

$$X = \omega a_1 x + (\omega-1)y + (2\omega+1)a_3 z,$$
$$Y = -(\omega+1)a_1 x - (\omega+2)y - (2\omega+1)a_3 z,\ Z = x$$

   is isomorphic over $\mathbb{F}(\omega)$ to the generalized Hessian curve $\mathbf{H}_{c,d}$ with $c = {a_1}^3 - 27a_3$ and $d = 3a_1$. On the other hand, the generalized Hessian curve $\mathbf{H}_{c,d}$ is isomorphic over $\mathbb{F}(\omega)$ to the Weierstraß curve $\mathbf{E}_{a_1,a_3}$ with $a_1 = d/3$, $a_3 = (d^3 - 27c)/3^6$.
2. If $p = 3$, the elliptic curve $\mathbf{E}_{a_1,a_3}$ via the map $(x,y,z) \mapsto (X,Y,Z)$ given by

$$X = -{a_3}^2 z,\ Y = a_3(a_1 x + y + a_3 z),\ Z = -y$$

   is isomorphic over $\mathbb{F}$ to the generalized Hessian curve $\mathbf{H}_{c,d}$ with $c = {a_3}^3$ and $d = {a_1}^3$. Conversely, every generalized Hessian curve $\mathbf{H}_{c,d}$ is isomorphic over $\mathbb{F}$ to the Weierstraß curve $\mathbf{E}_{a_1,a_3}$ with $a_1 = \sqrt[3]{d}$, $a_3 = \sqrt[3]{c}$. □

Remark 1. Consider the elliptic curve $\mathbf{E}_{a_1,a_3}$ defined in the proof of Theorem 1. If $p \neq 3$ and ${a_1}^3 - 27a_3$ is a cube in $\mathbb{F}$, we let $c = 1$ and $d = 3(a_1+2\delta)/(a_1-\delta)$, where $\delta^3 = {a_1}^3 - 27a_3$. Then, the map $(x,y,z) \mapsto (X,Y,Z)$ given by

$$X = (2a_1+\delta)x + 3y + 3a_3 z,\ Y = -(a_1-\delta)x - 3y,\ Z = -(a_1-\delta)x - 3a_3 z$$

is an isomorphism over $\mathbb{F}$ between $\mathbf{E}_{a_1,a_3}$ and $\mathbf{H}_{c,d}$.

Theorem 2. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then, the group $E(\mathbb{F}_q)$ has a point of order 3 if and only if E is isomorphic over $\mathbb{F}_q$ to a generalized Hessian curve.*

Proof. If $q \equiv 0, 1 \pmod 3$ then the theorem is a direct consequence of Theorem 1.

Next, we assume that $q \equiv 2 \pmod 3$. So, every element of $\mathbb{F}_q$ is a cube. If the elliptic curve E has an $\mathbb{F}_q$-rational point of order 3 then Remark 1 provides an isomorphism between E and a generalized Hessian curve. Moreover, every generalized Hessian curve $\mathbf{H}_{c,d}$ over $\mathbb{F}_q$ has the point $(-\zeta : 0 : 1)$ of order 3, where $\zeta^3 = c$ (see Section 4). □

3 Unified Addition Formulas

Let $\mathbf{H}_{c,d}$ be a generalized Hessian curve over $\mathbb{F}$. We recall that the addition formulas (5) do not work to double a point. Hereafter, we give some *unified* addition formulas for $\mathbf{H}_{c,d}$ where the doubling formulas can be derived directly from the addition formulas. The unified addition formulas make generalized Hessian curves interesting against side-channel attacks [2, 9].

Let $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ be two points of $\mathbf{H}_{c,d}(\mathbb{F})$. Let also $T = (-\zeta : 0 : 1) \in \mathbf{H}_{c,d}(\overline{\mathbb{F}})$ with $\zeta^3 = c$. Letting $Q_1 = P_1 + T$ and $Q_2 = P_2 - T$, we have $Q_1 = (\zeta Y_1 : \zeta^2 Z_1 : X_1)$ and $Q_2 = (\zeta^2 Z_2 : \zeta X_2 : Y_2)$. Clearly, $P_1 + P_2 = Q_1 + Q_2$. To compute $P_1 + P_2$, we use the addition formulas (5) with inputs Q_1 and Q_2. Doing so, we see that the sum of the points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ on $\mathbf{H}_{c,d}$ is the point $(X_3 : Y_3 : Z_3)$ given by

$$X_3 = cY_2Z_2{Z_1}^2 - X_1Y_1{X_2}^2, \quad Y_3 = X_2Y_2{Y_1}^2 - cX_1Z_1{Z_2}^2,$$
$$Z_3 = X_2Z_2{X_1}^2 - Y_1Z_1{Y_2}^2 \ . \quad (9)$$

These formulas work for doubling, i.e., they are unified addition formulas. We note that, by the swapping the order of the points in the addition formulas (9), one can obtain the following unified formulas:

$$X_3 = cY_1Z_1{Z_2}^2 - X_2Y_2{X_1}^2, \quad Y_3 = X_1Y_1{Y_2}^2 - cX_2Z_2{Z_1}^2,$$
$$Z_3 = X_1Z_1{X_2}^2 - Y_2Z_2{Y_1}^2 \ . \quad (10)$$

The next algorithm evaluates the addition formulas (9) with $12\mathbf{M} + 1\mathbf{D}$, where $1\mathbf{D}$ denotes the multiplication by constant c, which may be chosen small:

$$A = X_1X_2,\ B = Y_1Y_2,\ C = cZ_1Z_2,\ D = X_1Z_2,\ E = Y_1X_2,\ F = Z_1Y_2,$$
$$X_3 = CF - AE, \quad Y_3 = BE - CD, \quad Z_3 = AD - BF \ . \quad (11)$$

It turns out that a mixed addition requires $10\mathbf{M} + 1\mathbf{D}$ by setting $Z_2 = 1$. Moreover, the addition formulas (9) can be performed in a parallel way, similarly to the algorithm proposed for the addition formulas (5) in [33].

When $\mathbb{F}$ is of characteristic $p \neq 2$, one can use the modified system of coordinates presented in [22, §2.4]. Applying it to addition formulas (9), the sum of two points on $\mathbf{H}_{c,d}$ represented by $(X_1 : Y_1 : Z_1 : A_1 : B_1 : C_1 : D_1 : E_1 : F_1)$ and $(X_2 : Y_2 : Z_2 : A_2 : B_2 : C_2 : D_2 : E_2 : F_2)$ with

$$A_1 = {X_1}^2,\ B_1 = {Y_1}^2,\ C_1 = {Z_1}^2,\ D_1 = 2X_1Y_1,\ E_1 = 2X_1Z_1,\ F_1 = 2Y_1Z_1,$$
$$A_2 = {X_2}^2,\ B_2 = {Y_2}^2,\ C_2 = {Z_2}^2,\ D_2 = 2X_2Y_2,\ E_2 = 2X_2Z_2,\ F_2 = 2Y_2Z_2,$$

is the point represented by $(X_3 : Y_3 : Z_3 : A_3 : B_3 : C_3 : D_3 : E_3 : F_3)$ given by

$$X_3 = cC_1F_2 - D_1A_2,\ Y_3 = B_1D_2 - cE_1C_2,\ Z_3 = A_1E_2 - F_1B_2,$$
$$A_3 = {X_3}^2,\ B_3 = {Y_3}^2,\ C_3 = {Z_3}^2,\ D_3 = (X_3 + Y_3)^2 - A_3 - B_3, \quad (12)$$
$$E_3 = (X_3 + Z_3)^2 - A_3 - C_3,\ F_3 = (Y_3 + Z_3)^2 - B_3 - C_3 \ .$$

This algorithm requires $6\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$, where $2\mathbf{D}$ represent the two multiplications by constant c, which can be chosen small. Furthermore, the mixed addition formulas can be obtained by setting $Z_2 = 1$ which need $5\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$.

4 Complete Addition Formulas

Again, we let $\mathbf{H}_{c,d}$ denote a generalized Hessian curve over $\mathbb{F}$. In this section, we study the exceptional cases of the addition formulas (5), (9) and (10). In particular, we show that addition formulas (9), (10) work for all pairs of $\mathbb{F}$-rational points on $\mathbf{H}_{c,d}$ whenever c is not a cube in $\mathbb{F}$.

We consider the set of $\overline{\mathbb{F}}$-rational points at infinity on $\mathbf{H}_{c,d}$, denoted by ∞,

$$\infty = \left\{(1 : -\omega : 0) \mid \omega \in \overline{\mathbb{F}},\ \omega^3 = 1\right\} \ .$$

We note that ∞ is a subgroup of the group of $\overline{\mathbb{F}}$-rational points on $\mathbf{H}_{c,d}$. Further, ∞ is a subgroup of the 3-torsion group $\mathbf{H}_{c,d}[3]$, where

$$\mathbf{H}_{c,d}[3] = \left\{P \mid P \in \mathbf{H}_{c,d}(\overline{\mathbb{F}}),\ 3P = \mathcal{O}\right\} \ .$$

Let $\mathcal{T}_1$, $\mathcal{T}_2$ be the set of $\overline{\mathbb{F}}$-rational points $P = (X : Y : Z)$ of $\mathbf{H}_{c,d}[3]$ with $Y = 0$, $X = 0$, respectively. Namely,

$$\mathcal{T}_1 = \left\{(-\zeta : 0 : 1) \mid \zeta \in \overline{\mathbb{F}},\ \zeta^3 = c\right\} \quad \text{and} \quad \mathcal{T}_2 = \{-P \mid P \in \mathcal{T}_1\} \ .$$

Clearly, $\mathbf{H}_{c,d}[3]$ is partitioned into $\infty \cup \mathcal{T}_1 \cup \mathcal{T}_2$.

The following proposition describes the exceptional cases of the addition formulas (5).

Proposition 1. *The addition formulas* (5) *work for all pairs of points* P_1, P_2 *on* $\mathbf{H}_{c,d}$ *if and only if* $P_1 - P_2$ *is not a point at infinity.*

Proof. Let $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ be points in $\mathbf{H}_{c,d}(\overline{\mathbb{F}})$.

First, assume that the addition formulas (5) do not work for the inputs P_1, P_2, i.e., we have $X_3 = Y_3 = Z_3 = 0$, where $X_3 = X_2Z_2{Y_1}^2 - X_1Z_1{Y_2}^2$, $Y_3 = Y_2Z_2{X_1}^2 - Y_1Z_1{X_2}^2$ and $Z_3 = X_2Y_2{Z_1}^2 - X_1Y_1{Z_2}^2$. We distinguish two cases to show that $P_1 - P_2 \in \infty$.

1. If $Z_1 = 0$ then $Z_3 = -X_1Y_1{Z_2}^2$. We see that $X_1Y_1 \neq 0$, since $P_1 \in \mathbf{H}_{c,d}$. So, $Z_2 = 0$. That means P_1, P_2 are in ∞. Therefore, $P_1 - P_2$ is a point at infinity.
2. Assume now that $Z_1 \neq 0$ and $Z_2 \neq 0$. We write $P_1 = (x_1 : y_1 : 1)$ and $P_2 = (x_2 : y_2 : 1)$, where $x_i = X_i/Z_i$ and $y_i = Y_i/Z_i$ $(i = 1, 2)$. From $X_3 = Y_3 = Z_3 = 0$, we have ${x_2}{y_1}^2 = {x_1}{y_2}^2$, ${y_2}{x_1}^2 = {y_1}{x_2}^2$ and $x_1y_1 = x_2y_2$. So, $y_1y_2({x_1}^3 - {x_2}^3) = 0$ and $x_1x_2({y_1}^3 - {y_2}^3) = 0$. Moreover, from the equation of $\mathrm{H}_{c,d}$, we have ${x_1}^3 + {y_1}^3 = {x_2}^3 + {y_2}^3$.
   If $x_1x_2 \neq 0$ then ${y_1}^3 = {y_2}^3$. Next, we assume that $x_1x_2 = 0$. If $x_1 = 0$ then $y_1 \neq 0$. From $X_3 = 0$, we remark that $x_2 = 0$. Then, $x_1 = x_2 = 0$

implies that ${y_1}^3 = {y_2}^3$. Therefore, in all cases, we obtain ${y_1}^3 = {y_2}^3$ and ${x_1}^3 = {x_2}^3$. So, we can write $y_2 = \omega_1 y_1$ and $x_2 = \omega_2 x_1$, where ω_1, ω_2 are third roots of unity. The condition $x_1 y_1 = x_2 y_2$ becomes $(\omega_1\omega_2 - 1)x_1 y_1 = 0$. If $x_1 y_1 \neq 0$ then $\omega_2 = {\omega_1}^{-1}$ and thus $P_1 - P_2 = (1 : -\omega_1 : 0)$. If $x_1 = 0$ then $x_2 = 0$ and $P_1 - P_2 = (1 : -\omega_1 : 0)$. Finally, if $y_1 = 0$ then $y_2 = 0$ and $P_1 - P_2 = (\omega_2 : -1 : 0)$. Summing up, we always have $P_1 - P_2 \in \infty$.

Now, we study the other direction. We assume that $P_1 - P_2 \in \infty$ where $P_1, P_2 \in \mathbf{H}_{c,d}(\overline{\mathbb{F}})$. Then $P_1 = P_2 + (1 : -\omega : 0) = (\omega X_2 : \omega^{-1} Y_2 : Z_2)$, where ω is a third root of unity. It is easily seen that the addition formulas (5) do not work for such P_1, P_2. □

We note that the addition formulas (5) work for all *distinct* pairs of $\mathbb{F}$-rational inputs if the curve $\mathbf{H}_{c,d}$ over $\mathbb{F}$ has only one $\mathbb{F}$-rational point at infinity, i.e., if $\mathbb{F}$ has only one third root of unity. This happens for Hessian curves $\mathbf{H}_{c,d}$ over $\mathbb{F}_q$ with $q \not\equiv 1 \pmod 3$ and, in particular, for binary curves $\mathbf{H}_{c,d}$ over $\mathbb{F}_{2^n}$ with odd integers n.

Proposition 2. *The addition formulas* (9) *work for all pairs of points* P_1, P_2 *on* $\mathbf{H}_{c,d}$ *if and only if* $P_1 - P_2 \notin \mathcal{T}_1$.

Proof. Let P_1, P_2 be points on $\mathbf{H}_{c,d}$. Let T_1 be a point of $\mathcal{T}_1$. Let $Q_1 = P_1 + T_1$ and $Q_2 = P_2 - T_1$. We note that the output of formulas (9) for the pair of points P_1, P_2 is equal to the output of formulas (5) for the pair of points Q_1, Q_2. From Proposition 1, we see that the formulas (9) do not work for the pair of points P_1, P_2 if and only if $Q_1 - Q_2 \in \infty$. This is equivalent to $P_1 - P_2 \in \mathcal{T}_1$. □

Similarly, the addition formulas (10) work for all pairs of points P_1, P_2 on $\mathbf{H}_{c,d}$ with $P_1 - P_2 \notin \mathcal{T}_2$. Since the sets $\mathcal{T}_1$ and $\mathcal{T}_2$ are disjoint, if the addition formulas (9) fail to compute the sum of two points, then the addition formulas (10) work to compute this sum. Clearly, this is true for the other way round. In other words, if the addition formulas (9) do not work for the pair of inputs P_1, P_2, then they work for the pair of inputs P_2, P_1.

Corollary 1. *The doubling formulas* (6) *for the generalized Hessian curve* $\mathbf{H}_{c,d}$ *work for all inputs.*

Proof. The doubling formulas (6) can be obtained from the addition formulas (9) by letting $P_2 = P_1$. Then, from Proposition 2, we see that these doubling formulas work for all points on $\mathbf{H}_{c,d}$. □

Corollary 2. *Assume* $\mathcal{H}$ *is a subgroup of* $\mathbf{H}_{c,d}(\overline{\mathbb{F}})$ *which is disjoint from* $\mathcal{T}_1$. *Then, the addition formulas* (9) *and* (10) *work for all pairs of points in* $\mathcal{H}$.

Proof. Clearly, $\mathcal{H}$ and $\mathcal{T}_2$ are disjoint as well. Then, Proposition 2 concludes the proof. □

Here, we express the family of *complete generalized Hessian* curves. By a *complete* curve, we mean a curve with complete addition formulas, i.e., a curve over a field $\mathbb{F}$ with addition formulas that are valid for every pair of $\mathbb{F}$-rational points.

Theorem 3. *Let c, d be elements of $\mathbb{F}$ such that $d^3 \neq 27c$. Let $\mathbf{H}_{c,d}$ be the generalized Hessian curve over $\mathbb{F}$ with the addition formulas* (9)*. Then, $\mathbf{H}_{c,d}$ is complete over $\mathbb{F}$ if and only if c is not a cube in $\mathbb{F}$.*

Proof. By definition of $\mathcal{T}_1$, we see that the set of $\mathbb{F}$-rational points of $\mathcal{T}_1$ is empty if and only if c is not a cube in $\mathbb{F}$. By Proposition 2, the addition formulas (9) work for all pairs of $\mathbb{F}$-rational points if and only if the set of $\mathbb{F}$-rational points of $\mathcal{T}_1$ is empty, which completes the proof. □

Below, we give two examples of generalized Hessian curves over finite fields with complete addition formulas.

Example 1. Let c, d be elements of the finite field $\mathbb{F}_q$ with $q \equiv 1 \pmod 3$ such that $d^3 \neq 27c$ and c is not a cube in $\mathbb{F}_q$. Then, the generalized Hessian curve $\mathrm{H}_{c,d}$ over $\mathbb{F}_q$ is complete with the addition formulas (9) or (10).

Example 2. Let c, d be elements of $\mathbb{F}_q$ such that $c \neq 0$ and $d^3 \neq 27c$. Let $\mathcal{H}$ be a subgroup of $\mathbf{H}_{c,d}(\mathbb{F}_q)$ with $\gcd(\#\mathcal{H}, 3) = 1$. Then, $\mathcal{H}$ is complete over $\mathbb{F}_q$ with the addition formulas (9) or (10).

5 Explicit Formulas in Characteristic 2

In this section, we present fast and efficient addition, doubling, tripling and differential addition formulas for generalized binary Hessian curves over a field $\mathbb{F}$ of characteristic $p = 2$.

5.1 Addition

We recall that the cost of point addition algorithms in [13, 33] for the addition formulas (5) is 12**M**. Also, the addition algorithm (11) requires 12**M** + 1**D**. One may choose the constant c small to reduce the cost of this algorithm to 12**M**. Further, the addition algorithm (11) is *unified*. Furthermore, it features *completeness* for generalized binary Hessian curve $\mathbf{H}_{c,d}$ over $\mathbb{F}_{2^n}$, where n is even and c is not a cube in $\mathbb{F}_{2^n}$.

Moreover, one can use the extended coordinates $(X : Y : Z : X^2 : Y^2 : Z^2 : XY : XZ : YZ)$. Here, the sum of two points on $\mathbf{H}_{c,d}$ represented by $(X_1 : Y_1 : Z_1 : A_1 : B_1 : C_1 : D_1 : E_1 : F_1)$ and $(X_2 : Y_2 : Z_2 : A_2 : B_2 : C_2 : D_2 : E_2 : F_2)$ where

$$A_1 = {X_1}^2,\ B_1 = {Y_1}^2,\ C_1 = {Z_1}^2,\ D_1 = X_1Y_1,\ E_1 = X_1Z_1,\ F_1 = Y_1Z_1,$$
$$A_2 = {X_2}^2,\ B_2 = {Y_2}^2,\ C_2 = {Z_2}^2,\ D_2 = X_2Y_2,\ E_2 = X_2Z_2,\ F_2 = Y_2Z_2$$

is the point represented by $(X_3 : Y_3 : Z_3 : A_3 : B_3 : C_3 : D_3 : E_3 : F_3)$ given by

$$\begin{gathered} X_3 = cC_1F_2 + D_1A_2,\ Y_3 = B_1D_2 + cE_1C_2,\ Z_3 = A_1E_2 + F_1B_2, \\ A_3 = {X_3}^2,\ B_3 = {Y_3}^2,\ C_3 = {Z_3}^2,\ D_3 = X_3Y_3,\ E_3 = X_3Z_3,\ F_3 = Y_3Z_3\ . \end{gathered} \tag{13}$$

This algorithm requires $9\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$, where the two $\mathbf{D}$ are multiplication by the constant c. We note that the algorithm (13) is obtained from the addition formulas (9), so it is *unified* and works for point doublings as well. Moreover, it works for all pairs of inputs on a *complete* curve (cf. Theorem 3). Furthermore, the mixed addition formulas need $8\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$ by setting $Z_2 = 1$. If c is small, then one can obtain the addition algorithm in a parallel environment using $3, 4$ or 6 processors which needs $3\mathbf{M} + 1\mathbf{S}$, $3\mathbf{M}$ or $2\mathbf{M}$, respectively.

Table 1. Cost of addition formulas for different families of binary elliptic curves

Curve shape	Representation	Projective addition	Mixed addition
Short Weierstraß	Projective [4]	$14\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$	$11\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$
$y^2 + xy = x^3 + a_2x^2 + a_6$	Jacobian [4]	$14\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$	$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
	Lopez-Dahab [1, 4, 20]	$13\mathbf{M} + 4\mathbf{S}$	$8\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$
	Extended Lopez-Dahab		
	with $a_2 = 0$ [1, 4, 20]	$14\mathbf{M} + 3\mathbf{S}$	$9\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$
	with $a_2 = 1$ [1, 4, 20, 24]	$13\mathbf{M} + 3\mathbf{S}$	$8\mathbf{M} + 4\mathbf{S}$
Binary Edwards	Projective [6]	$18\mathbf{M} + 2\mathbf{S} + 7\mathbf{D}$	$13\mathbf{M} + 3\mathbf{S} + 3\mathbf{D}$
$d_1(x + y) + d_2(x^2 + y^2)$	Projective		
$= xy + xy(x + y) + x^2y^2$	with $d_1 = d_2$ [6]	$16\mathbf{M} + 1\mathbf{S} + 4\mathbf{D}$	$13\mathbf{M} + 3\mathbf{S} + 3\mathbf{D}$
Hessian	Projective [13, 23, 33]	$12\mathbf{M}$	$10\mathbf{M}$
$x^3 + y^3 + 1 = dxy$	Projective, formulas (11)	$12\mathbf{M}$	$10\mathbf{M}$
	Extended, formulas (13)	$9\mathbf{M} + 3\mathbf{S}$	$8\mathbf{M} + 3\mathbf{S}$
Generalized Hessian	Projective [12]	$12\mathbf{M}$	$10\mathbf{M}$
$x^3 + y^3 + c = dxy$	Projective, formulas (11)	$12\mathbf{M} + 1\mathbf{D}$	$10\mathbf{M} + 1\mathbf{D}$
	Extended, formulas (13)	$9\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$	$8\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$

Table 1 lists the complexities of addition formulas for different shapes of binary elliptic curves and different coordinate systems. As Table 1 shows, the generalized Hessian curves provide the fastest addition formulas for binary elliptic curves. Moreover, our formulas for Hessian curves are unified. They are even complete for many generalized Hessian curves. We note that all addition formulas for short Weierstraß curve are not even unified. But, binary Edwards curves provide unified and even complete formulas.

5.2 Doubling

We recall that the doubling algorithm (7) needs $6\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ to perform the doubling formulas (6). Furthermore, from the doubling formulas (6), we see that the doubling of the point $(X_1 : Y_1 : Z_1)$ on $\mathbf{H}_{c,d}$ is the point $(X_3 : Y_3 : Z_3)$ with

$$X_3 = {Y_1}^4 + dX_1{Y_1}^2Z_1,\ Y_3 = {X_1}^4 + d{X_1}^2Y_1Z_1,\ Z_3 = c{Z_1}^4 + dX_1Y_1{Z_1}^2\ . \quad (14)$$

The following algorithm performs the doubling formulas (14) which requires $5\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$:

$$A = {X_1}^2,\ B = {Y_1}^2,\ C = {Z_1}^2,\ D = X_1Y_1,\ G = DZ_1,\ H = dG,$$
$$X_3 = B^2 + Y_1H,\ Y_3 = A^2 + X_1H,\ Z_3 = cC^2 + Z_1H\ .$$

Moreover, the doubling of the point $(X_1 : Y_1 : Z_1)$ on a binary curve $\mathbf{H}_{c,d}$, using the representation $(X_1 : Y_1 : Z_1 : A_1 : B_1 : C_1 : D_1 : E_1 : F_1)$, where $A_1 = {X_1}^2$, $B_1 = {Y_1}^2$, $C_1 = {Z_1}^2$, $D_1 = X_1Y_1$, $E_1 = X_1Z_1$, $F_1 = Y_1Z_1$, is the point represented by $(X_3 : Y_3 : Z_3 : A_3 : B_3 : C_3 : D_3 : E_3 : F_3)$ given by

$$X_3 = B_1(B_1 + dE_1),\ Y_3 = A_1(A_1 + dF_1),\ Z_3 = (A_1 + B_1 + D_1)(E_1 + F_1),$$
$$A_3 = {X_3}^2,\ B_3 = {Y_3}^2,\ C_3 = {Z_3}^2,\ D_3 = X_3Y_3,\ E_3 = X_3Z_3,\ F_3 = Y_3Z_3\ .$$

The cost of above doubling algorithm is $6\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$. We also note that, the coordinates D_3, E_3 and F_3 can be given by

$$D_3 = {D_1}^4 + cd{E_1}^2{F_1}^2,\ E_3 = c{F_1}^4 + d{D_1}^2{E_1}^2,\ F_3 = c{E_1}^4 + d{D_1}^2{F_1}^2\ .$$

The following doubling algorithm needs less field multiplications:

$$G = {A_1}^2,\ H = {B_1}^2,\ I = {C_1}^2,\ J = D_1E_1,\ K = D_1F_1,\ L = E_1F_1,$$
$$X_3 = H + dK,\ Y_3 = G + dJ,\ Z_3 = cI + dL,\ A_3 = {X_3}^2,\ B_3 = {Y_3}^2,\ C_3 = {Z_3}^2,$$
$$R = {D_1}^2 + \sqrt{cd}L,\ S = \sqrt{c}{F_1}^2 + \sqrt{d}J,\ T = \sqrt{c}{E_1}^2 + \sqrt{d}K,$$
$$D_3 = R^2,\ E_3 = S^2,\ F_3 = T^2\ .$$

Above doubling algorithm needs $3\mathbf{M} + 12\mathbf{S} + 9\mathbf{D}$. This algorithm requires $3\mathbf{M} + 12\mathbf{S} + 6\mathbf{D}$ if c is small and $3\mathbf{M} + 12\mathbf{S} + 4\mathbf{D}$ if d is small.

Our doubling formulas slightly improve the current speed of doublings on Hessian curves. Moreover, the doubling formulas for generalized Hessian curves are faster than doubling formulas using projective coordinates in short Weierstraß form, see [2]. But, they are slower than various doubling formulas using Jacobian [2], Lopez-Dahab representations of short Weierstraß form [2, 29, 24, 6] and projective representation of binary Edwards [6].

We note that the only *complete* doubling formulas are presented by binary Edwards [6] and generalized binary Hessian curves (see Corollary 1).

5.3 Tripling

Here, we present fast tripling formulas for generalized binary Hessian curves. The tripling formulas can be used in double based number systems, DBNS; see e.g., [14, 3, 15]. For a point $(X_1 : Y_1 : Z_1)$ on $\mathbf{H}_{c,d}$, we have $3(X_1 : Y_1 : Z_1) = (X_3 : Y_3 : Z_3)$ with

$$X_3 = d({Y_1}^3({Z_1}^3 + {X_1}^3)({X_1}^3 + {Y_1}^3) + {X_1}^3({Y_1}^3 + {Z_1}^3)({Y_1}^3 + {Z_1}^3))\,,$$
$$Y_3 = d({X_1}^3({Y_1}^3 + {Z_1}^3)({X_1}^3 + {Y_1}^3) + {Y_1}^3({Z_1}^3 + {X_1}^3)({Z_1}^3 + {X_1}^3))\,,$$
$$Z_3 = ({X_1}^3 + {Y_1}^3 + {Z_1}^3)(({Y_1}^3 + {Z_1}^3)({Z_1}^3 + {X_1}^3) + ({X_1}^3 + {Y_1}^3)^2)\ .$$

For generalized binary Hessian curves, we suggest the following formulas. If $d \neq 0$, let $e = d^{-1}$. The following algorithm computes $(X_3 : Y_3 : Z_3)$ and requires $7\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ (and $7\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ if either c or e is small),

$$\begin{gathered} A = {X_1}^3,\ B = {Y_1}^3,\ C = c{Z_1}^3,\ E = A^2,\ F = B^2,\ G = C^2, \\ H = (A+C)(F+G),\ I = (B+C)(E+G),\ J = (A+B)(E+F), \\ K = (A+B+C)(E+F+G),\ L = H + I + (1+ce^3)K, \\ X_3 = H + J + L,\ Y_3 = I + J + L,\ Z_3 = eL\ . \end{gathered}$$

5.4 Differential addition

We now devise differential addition formulas on binary Hessian curves using w-coordinates, where for a point (x, y) on the binary curve $\mathrm{H}_{c,d}$, $w(x, y)$ is defined by a *symmetric* function in terms of the coordinates x, y.

The w-coordinates for differential addition require computing $w(P+Q)$ given $w(P)$, $w(Q)$ and $w(P-Q)$; and the w-coordinates for differential doubling require computing $w(2P)$ given $w(P)$. We recall, [31, 6], that using w-coordinate differential addition and doubling formulas, one can recursively compute $w((2m+1)P)$ and $w(2mP)$ given $w(mP)$ and $w((m+1)P)$.

Let (x_2, y_2) be a point on $\mathrm{H}_{c,d}$ and let $(x_4, y_4) = 2(x_2, y_2)$. Write $u_i = x_i + y_i$ and $v_i = x_i y_i$ for $i = 2, 4$. From doubling formulas (4), we obtain

$$u_4 = \frac{{u_2}^4 + cd}{d{u_2}^2 + c} \quad \text{and} \quad v_4 = \frac{{v_2}^4 + cd{v_2}^2}{d^2{v_2}^2 + c^2}\ . \tag{15}$$

Assume that $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_5, y_5)$ are affine points on $\mathrm{H}_{c,d}$ satisfying $(x_1, y_1) = (x_3, y_3) - (x_2, y_2)$ and $(x_5, y_5) = (x_2, y_2) + (x_3, y_3)$. Write $u_i = x_i + y_i$ and $v_i = x_i y_i$ for $i = 1, 2, 3, 5$. Using the addition formulas (3), we obtain

$$\begin{aligned} u_1 + u_5 &= \frac{{u_2}^2{u_3}^2 + du_2u_3(u_2+u_3) + d^2u_2u_3}{d({u_2}^2 + {u_3}^2) + u_2u_3(u_2+u_3+d) + c}\,, \\ u_1u_5 &= \frac{d{u_2}^2{u_3}^2 + c({u_2}^2 + {u_3}^2 + d^2)}{d({u_2}^2 + {u_3}^2) + u_2u_3(u_2+u_3+d) + c}\ . \end{aligned}$$

Furthermore, we have

$$\begin{aligned} v_1 + v_5 &= \frac{(c+dv_2)(c+dv_3)}{(v_2+v_3)^2}\,, \\ v_1v_5 &= \frac{{v_2}^2{v_3}^2 + cdv_2v_3 + c^2(v_2+v_3)}{(v_2+v_3)^2}\ . \end{aligned} \tag{16}$$

Using above affine formulas one can obtain fast projective and mixed differential addition and doubling formulas. In order to speed up these formulas, we consider the following w-coordinates. We write $w_i = c + dv_i$ for $i = 1, 2, \ldots, 5$. In other words, $w_i = {x_i}^3 + {y_i}^3$. Here, $d \neq 0$. From (15), we have

$$w_4 = \frac{{w_2}^4 + c^3(d^3 + c)}{d^3{w_2}^2}\ .$$

Using the formulas (16), we obtain

$$w_1 + w_5 = \frac{d^3 w_2 w_3}{(w_2 + w_3)^2} \quad \text{and} \quad w_1 w_5 = \frac{{w_2}^2 {w_3}^2 + c^3(d^3 + c)}{(w_2 + w_3)^2} \ .$$

To have projective formulas, we assume that w_i are given by the fractions W_i/Z_i for $i = 1, 2, 3$. The following explicit formulas give the output w_5 defined by W_5/Z_5:

$$\begin{gathered} A = W_2 Z_3,\ B = W_3 Z_2,\ C = AB,\ U = d^3 C,\ V = (A+B)^2, \\ Z_5 = Z_1 V,\ W_5 = Z_1 U + W_1 V \ . \end{gathered} \tag{17}$$

These formulas require $6\mathbf{M}+1\mathbf{S}+1\mathbf{D}$. Furthermore, the cost of mixed differential addition with w-coordinates is $4\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ by setting $Z_1 = 1$.

Moreover, we write w_4 by the fraction W_4/Z_4. Then, the explicit doubling formulas

$$\begin{gathered} A = {W_2}^2,\ B = {Z_2}^2,\ C = A + \sqrt{c^3(d^3 + c)}B,\ D = d^3 B, \\ W_4 = C^2,\ Z_4 = AD \end{gathered} \tag{18}$$

use $1\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$. If $c = 1$, i.e., $\mathbf{H}_{c,d}$ is a Hessian curve, then the explicit doubling formulas use $1\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$:

$$\begin{gathered} A = {W_2}^2,\ B = {Z_2}^2,\ C = A + B,\ D = (1/\sqrt{d^3})C, \\ W_4 = (B + D)^2,\ Z_4 = AB \ . \end{gathered} \tag{19}$$

As a result, the total cost of projective w-coordinate differential addition and doubling is $7\mathbf{M} + 4\mathbf{S} + 3\mathbf{D}$. Also, the mixed w-coordinate differential addition and doubling formulas use $5\mathbf{M} + 4\mathbf{S} + 3\mathbf{D}$. For Hessian curves $\mathbf{H}_{1,d}$, the total costs of projective and mixed w-coordinate differential addition and doubling are $7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ and $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$, respectively. Furthermore, if the parameter d of the curve $\mathbf{H}_{c,d}$ is chosen small then the total costs of projective and mixed w-coordinate differential addition and doubling reduces to $7\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ and $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, respectively. Moreover, from Proposition 1, we can see that the mixed w-coordinate addition and doubling formulas are *complete*.

Table 2 shows the cost of differential addition and doubling for different coordinate systems on binary elliptic curves. From Table 2, we see that our w-coordinate representations for generalized Hessian curves are competitive with other representations for binary elliptic curves.

6 Conclusion

In this paper, the family of *generalized Hessian curves* has been presented. This family covers more isomorphism classes of elliptic curves than Hessian curves. For every elliptic curve E over a finite field $\mathbb{F}_q$, the group $E(\mathbb{F}_q)$ has a point of order 3 if and only if E is isomorphic over $\mathbb{F}_q$ to a generalized Hessian curve.

Unified addition formulas have been presented for generalized Hessian curves $\mathbf{H}_{c,d}$ over a field $\mathbb{F}$, see formulas (9), (10). In particular, these formulas are unified

Table 2. Cost of differential addition and doubling for families of binary elliptic curves

Curve shape	Representation	Projective differential addition+doubling	Mixed differential addition+doubling
Short Weierstraß	$XZ(x=X/Z)$[28]	$7\mathbf{M}+5\mathbf{S}+1\mathbf{D}$	$5\mathbf{M}+5\mathbf{S}+1\mathbf{D}$
$y^2+xy=x^3+a_2x^2+a_6$	$XZ(x=X/Z)$[18]	$6\mathbf{M}+5\mathbf{S}+1\mathbf{D}$	$5\mathbf{M}+5\mathbf{S}+1\mathbf{D}$
	$XZ(x=X/Z)$[34, §3.1]	$7\mathbf{M}+4\mathbf{S}+1\mathbf{D}$	$5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$
	$XZ(x=X/Z)$[34, §3.2]	$6\mathbf{M}+5\mathbf{S}+2\mathbf{D}$	$5\mathbf{M}+5\mathbf{S}+2\mathbf{D}$
Binary Edwards			
$d_1(x+y)+d_2(x^2+y^2)$	$WZ(x+y=W/Z)$ [6]	$8\mathbf{M}+4\mathbf{S}+4\mathbf{D}$	$6\mathbf{M}+4\mathbf{S}+4\mathbf{D}$
$=xy+xy(x+y)+x^2y^2$	WZ with $d_1=d_2$ [6]	$7\mathbf{M}+4\mathbf{S}+2\mathbf{D}$	$5\mathbf{M}+4\mathbf{S}+2\mathbf{D}$
Hessian	$WZ(1+dxy=W/Z)$		
$x^3+y^3+1=dxy$	formulas (17), (19)	$7\mathbf{M}+4\mathbf{S}+2\mathbf{D}$	$5\mathbf{M}+4\mathbf{S}+2\mathbf{D}$
Generalized Hessian	$WZ(c+dxy=W/Z)$		
$x^3+y^3+c=dxy$	formulas (17), (18)	$7\mathbf{M}+4\mathbf{S}+3\mathbf{D}$	$5\mathbf{M}+4\mathbf{S}+3\mathbf{D}$
	WZ with small d		
	formulas (17), (18)	$7\mathbf{M}+4\mathbf{S}+1\mathbf{D}$	$5\mathbf{M}+4\mathbf{S}+1\mathbf{D}$

for Hessian curves $\mathbf{H}_{1,d}$. Further, the formulas are *complete* if c is not a cube in $\mathbb{F}$.

The cost of projective formulas using algorithm (11) is $12\mathbf{M}+1\mathbf{D}$. Also, the mixed addition formulas require $10\mathbf{M}+1\mathbf{D}$. For generalized Hessian curves $\mathbf{H}_{c,d}$ over $\mathbb{F}$ with characteristic $p \neq 2$, the projective addition formulas (12) using extended coordinates has a cost of $6\mathbf{M}+6\mathbf{S}+2\mathbf{D}$. The mixed formulas require $5\mathbf{M}+5\mathbf{S}+2\mathbf{D}$.

When $p=2$, the generalized binary Hessian curves provide very fast and efficient addition formulas. Projective formulas (11) require $12\mathbf{M}+1\mathbf{D}$ and the mixed addition formulas need $10\mathbf{M}+1\mathbf{D}$. Moreover, using the extended coordinates, formulas (13) perform a projective addition using $9\mathbf{M}+3\mathbf{S}+2\mathbf{D}$ and a mixed addition using $8\mathbf{M}+3\mathbf{S}+2\mathbf{D}$. Several doubling and tripling formulas have been presented for generalized Hessian curves which improve the previous doubling and tripling formulas on Hessian curves. Also, very competitive differential addition and doubling formulas have been presented for generalized binary Hessian curves.

References

1. E. Al-Daoud, R. Mahmod, M. Rushdan, and A. Kiliçman. A new addition formula for elliptic curves over GF(2^n). *IEEE Trans. Computers*, 51(8):972–975, 2002.
2. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* CRC Press, 2005.
3. R. M. Avanzi, V. S. Dimitrov, C. Doche, and F. Sica. Extending scalar multiplication using double bases. In X. Lai and K. Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 130–144. Springer, 2006.
4. D. J. Bernstein and T. Lange. Explicit-formulas database. `http://www.hyperelliptic.org/EFD/`.

5. D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 29–50. Springer, 2007.
6. D. J. Bernstein, T. Lange, and R. R. Farashahi. Binary Edwards curves. In E. Oswald and P. Rohatgi, editors, *CHES 2008*, volume 5154 of *LNCS*, pages 244–265. Springer, 2008.
7. D. J. Bersntein, D. Kohel, and T. Lange. Twisted Hessian curves. `http://www.hyperelliptic.org/EFD/g1p/auto-twistedhessian.html`.
8. O. Billet and M. Joye. The Jacobi model of an elliptic curve and side-channel analysis. In M. P. C. Fossorier, T. Høholdt, and A. Poli, editors, *AAECC-15*, volume 2643 of *LNCS*, pages 34–42. Springer, 2003.
9. I. F. Blake, G. Seroussi, and N. P. Smart. *Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.
10. É. Brier, I. Déchène, and M. Joye. Unified point addition formulæ for elliptic curve cryptosystems. In *Embedded Cryptographic Hardware: Methodologies & Architectures*, pages 247–256. Nova Science Publishers, 2004.
11. É. Brier and M. Joye. Weierstraß elliptic curves and side-channel attacks. In D. Naccache and P. Paillier, editors, *PKC 2002*, volume 2274 of *LNCS*, pages 335–345. Springer, 2002.
12. J. W. S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.
13. D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986.
14. V. S. Dimitrov, L. Imbert, and P. K. Mishra. Efficient and secure elliptic curve point multiplication using double-base chains. In B. K. Roy, editor, *ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 59–78. Springer, 2005.
15. C. Doche and L. Imbert. Extended double-base number system with applications to elliptic curve cryptography. In R. Barua and T. Lange, editors, *INDOCRYPT 2006*, volume 4329 of *LNCS*, pages 335–348. Springer, 2006.
16. R. R. Farashahi. On the number of distinct Legendre, Jacobi and Hessian curves. Preprint.
17. R. R. Farashahi and I. E. Shparlinski. On the number of distinct elliptic curves in some families. *Designs, Codes and Cryptography*, 54(1):83–99, 2010.
18. P. Gaudry and D. Lubicz. The arithmetic of characteristic 2 Kummer surfaces. *Finite Fields and Applications*, 15:246–260, 2009.
19. O. Hesse. Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. *Journal für die reine und angewandte Mathematik*, 10:68–96, 1844.
20. A. Higuchi and N. Takagi. A fast addition algorithm for elliptic curve arithmetic in GF(2^n) using projective coordinates. *Inf. Process. Lett.*, 76(3):101–103, 2000.
21. H. Hisil, G. Carter, and E. Dawson. New formulæ for efficient elliptic curve arithmetic. In K. Srinathan, C. P. Rangan, and M. Yung, editors, *INDOCRYPT 2007*, volume 4859 of *LNCS*, pages 138–151. Springer, 2007.
22. H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson. Faster group operations on elliptic curves. In L. Brankovic and W. Susilo, editors, *Australasian Information Security Conference (AISC 2009)*, volume 98, pages 7–19. Conferences in Research and Practice in Information Technology (CRPIT), 2009.
23. M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 402–410. Springer, 2001.

24. K. H. Kim and S. I. Kim. A new method for speeding up arithmetic on elliptic curves over binary fields. Cryptology ePrint Archive, Report 2007/181, 2007.
25. A. Knapp. *Elliptic Curves*. Princeton University Press, 1992.
26. N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.
27. P.-Y. Liardet and N. P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 391–401. Springer, 2001.
28. J. López and R. Dahab. Fast multiplication on elliptic curves over GF(2^n) without precomputation. In Ç. K. Koç and C. Paar, editors, *CHES '99*, volume 1717 of *LNCS*, pages 316–327. Springer, 1999.
29. J. López and R. Dahab. Improved algorithms for elliptic curve arithmetic in GF(2^n). In S. E. Tavares and H. Meijer, editors, *SAC '98*, volume 1556 of *LNCS*, pages 201–212. Springer, 1999.
30. V. S. Miller. Use of elliptic curves in cryptography. In H. C. Williams, editor, *CRYPTO '85*, volume 218 of *LNCS*, pages 417–426. Springer, 1986.
31. P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.
32. J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.
33. N. P. Smart. The Hessian form of an elliptic curve. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 118–125. Springer, 2001.
34. M. Stam. On Montgomery-like representationsfor elliptic curves over GF(2^n). In Y. Desmedt, editor, *Public Key Cryptography*, volume 2567 of *LNCS*, pages 240–253. Springer, 2002.
35. L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC Press, 2005.

A On the Number of Distinct Generalized Hessian Curves

A.1 The number of distinct j-invariants

We recall from [16] that the number of distinct Hessian curves over the finite field $\mathbb{F}_q$, up to isomorphism over $\overline{\mathbb{F}}_q$, is $q-1$, $\lfloor (q+11)/12 \rfloor$ and $\lfloor q/2 \rfloor$ if $q \equiv 0, 1, 2 \pmod 3$, respectively. Using the similar method described in [16, 17], we give explicit formulas for the number of distinct generalized Hessian curves over the finite field $\mathbb{F}_q$ up to isomorphism over $\overline{\mathbb{F}}_q$.

From Equation (2), the j-invariant of $\mathrm{H}_{c,d}$ is $j(\mathrm{H}_{c,d}) = \frac{1}{c}\left(\frac{d(d^3+216c)}{d^3-27c}\right)^3$. We use J_{H} to denote the set of distinct j-invariants of the family of generalized Hessian curves over $\mathbb{F}_q$ and we let $J_{\mathrm{H}}(q) = \#J_{\mathrm{H}}$. For c in $\mathbb{F}_q$, with $c \neq 0$, we let

$$J_{\mathrm{H}_c} = \left\{ j \mid j = j(\mathrm{H}_{c,d}),\ d \in \mathbb{F}_q, d^3 \neq 27c \right\} \ .$$

Clearly, $J_{\mathrm{H}} = \bigcup_{c \in \mathbb{F}_q^*} J_{\mathrm{H}_c}$.

Lemma 1. *Let $c_1, c_2 \in \mathbb{F}_q^*$ and let $c = c_1/c_2$. If c is a cube in $\mathbb{F}_q$, then $J_{\mathrm{H}_{c_1}} = J_{\mathrm{H}_{c_2}}$. If c is not a cube in $\mathbb{F}_q$, then we have $J_{\mathrm{H}_{c_1}} \cap J_{\mathrm{H}_{c_2}} = \{0\}$.*

Proof. Suppose $c = \zeta^3$ is a cube in $\mathbb{F}_q$. For all $d \in \mathbb{F}_q$ with $d^3 \neq 27c$, we have $j(\mathrm{H}_{c_1,d}) = j(\mathrm{H}_{c_2,d/\zeta})$ and similarly $j(\mathrm{H}_{c_2,d}) = j(\mathrm{H}_{c_1,\zeta d})$. Therefore, $J_{\mathrm{H}_{c_1}} = J_{\mathrm{H}_{c_2}}$.

Now, suppose that c is not a cube in $\mathbb{F}_q$. Let $j \in J_{\mathrm{H}_{c_1}} \cap J_{\mathrm{H}_{c_2}}$. Then, $j = \frac{1}{c_1}\left(\frac{d_1(d_1{}^3+216c_1)}{d_1{}^3-27c_1}\right)^3 = \frac{1}{c_2}\left(\frac{d_2(d_2{}^3+216c_2)}{d_2{}^3-27c_2}\right)^3$ for some $d_1, d_2 \in \mathbb{F}_q$. If $j \neq 0$, we see that $c = c_1/c_2$ is a cube in $\mathbb{F}_q$, a contradiction. So, $J_{\mathrm{H}_{c_1}} \cap J_{\mathrm{H}_{c_2}} = \{0\}$. □

Lemma 2. *For $q \equiv 1 \pmod 3$, if c is not a cube in $\mathbb{F}_q$, we have $\#J_{\mathrm{H}_c} = (q+2)/3$.*

Proof. For $d \in \mathbb{F}_q$ with $d^3 \neq 27c$, we let $j(\mathrm{H}_{c,d}) = \frac{1}{c}\ (F(d))^3$ where $F(U) = \frac{U(U^3+216c)}{U^3-27c}$. We consider the bivariate rational function $F(U)-F(V)$. We obtain

$$F(U) - F(V) = \frac{U-V}{U^3-27c}\ \prod_{i=1}^{3}\left(U - \frac{3\zeta_i(V+6\zeta_i)}{V-3\zeta_i}\right),$$

where, $\zeta_1, \zeta_2, \zeta_3$ are three cubic roots of c in $\overline{\mathbb{F}}_q$. For all $u, v \in \mathbb{F}_q$ with $u^3 \neq 27c$, $v^3 \neq 27c$, we see that $F(u) = F(v)$ if and only if $u = v$. Hence, F is injective over $\mathbb{F}_q$ and we have $F(\mathbb{F}_q) = \mathbb{F}_q$. Now, consider the map $\kappa : \mathbb{F}_q^* \to \mathbb{F}_q^*$ by $\kappa(x) = \frac{1}{c}x^3$. This map is $3:1$, if $q \equiv 1 \pmod 3$. So, $\#J_{\mathrm{H}_c} = (q-1)/3 + 1$. □

Theorem 4. *For any prime power q, for the number $J_{\mathrm{H}}(q)$ of distinct values of the j-invariant of the family of generalized Hessian curves over the finite field $\mathbb{F}_q$, we have*

$$J_{\mathrm{H}}(q) = \begin{cases} q-1, & \text{if } q \equiv 0 \pmod 3 \\ \lfloor (3q+1)/4 \rfloor, & \text{if } q \equiv 1 \pmod 3 \\ \lfloor q/2 \rfloor, & \text{if } q \equiv 2 \pmod 3 \end{cases}.$$

Proof. If $q \not\equiv 1 \pmod 3$, every element of $\mathbb{F}_q$ is a cube in $\mathbb{F}_q$. Next, Lemma 1 implies that, for all $c \in \mathbb{F}_q^*$, we have $J_{\mathrm{H}_c} = J_{\mathrm{H}_1}$. Therefore, $J_{\mathrm{H}} = J_{\mathrm{H}_1}$. Then, from [16, Theorem 14], we have

$$J_{\mathrm{H}}(q) = \begin{cases} q-1, & \text{if } q \equiv 0 \pmod 3 \\ \lfloor q/2 \rfloor, & \text{if } q \equiv 2 \pmod 3 \end{cases}.$$

For $q \equiv 1 \pmod 3$, we fix a value $c \in \mathbb{F}_q$ that is not a cube in $\mathbb{F}_q$. Following Lemma 1, we write $J_{\mathrm{H}} = J_{\mathrm{H}_c} \cup J_{\mathrm{H}_{c^2}} \cup J_{\mathrm{H}_1}$, where $J_{\mathrm{H}_c} \cap J_{\mathrm{H}_{c^2}} = J_{\mathrm{H}_c} \cap J_{\mathrm{H}_1} = J_{\mathrm{H}_{c^2}} \cap J_{\mathrm{H}_1} = \{0\}$. By Lemma 2, we have $\#J_{\mathrm{H}_c} = \#J_{\mathrm{H}_{c^2}} = (q+2)/3$. Moreover, from [16, Theorem 14], we have

$$\#J_{\mathrm{H}_1} = \begin{cases} (q+11)/12, & \text{if } q \equiv 1 \pmod{12} \\ (q+8)/12, & \text{if } q \equiv 4 \pmod{12} \\ (q+5)/12, & \text{if } q \equiv 7 \pmod{12} \end{cases}.$$

Therefore, we have

$$J_{\mathrm{H}}(q) = \begin{cases} (3q+1)/4, & \text{if } q \equiv 1 \pmod{12} \\ 3q/4, & \text{if } q \equiv 4 \pmod{12} \\ (3q-1)/4, & \text{if } q \equiv 7 \pmod{12} \end{cases},$$

which completes the proof. □

A.2 The number of $\mathbb{F}_q$-isomorphism classes

We recall from [16] that the number of $\mathbb{F}_q$-isomorphism classes of Hessian curves over $\mathbb{F}_q$ is $\lfloor (q+11)/12 \rfloor$ if $q \equiv 1 \pmod 3$ and $q-1$ if $q \not\equiv 1 \pmod 3$. The following theorem gives explicit formulas for the number of distinct generalized Hessian curves, up to $\mathbb{F}_q$-isomorphism, over the finite field $\mathbb{F}_q$.

Theorem 5. *For any prime power q, the number of $\mathbb{F}_q$-isomorphism classes of the family of generalized Hessian curves over the finite field $\mathbb{F}_q$ is*

$$\begin{cases} \lfloor (3(q+3)/4 \rfloor, & \text{if } q \equiv 1 \pmod 3 \\ q-1, & \text{if } q \equiv 0,2 \pmod 3 \end{cases}.$$

Proof. We use $I_{\mathrm{H}}(q)$ to denote the number of $\mathbb{F}_q$-isomorphism classes of the family of generalized Hessian curves over $\mathbb{F}_q$.

If $q \equiv 0,2 \pmod 3$, then every generalized Hessian curve is $\mathbb{F}_q$-isomorphic to a Hessian curve via the map given by Equations (1). So, $I_{\mathrm{H}}(q)$ equals the number of $\mathbb{F}_q$-isomorphism classes of the family of Hessian curves over $\mathbb{F}_q$. Then, from [16, Theorem 15], we have $I_{\mathrm{H}}(q) = q-1$ if $q \not\equiv 1 \pmod 3$.

Now, suppose that $q \equiv 1 \pmod 3$. For $a \in \mathbb{F}_q$, let $i_H(a)$ be the set of $\mathbb{F}_q$-isomorphism classes of generalized Hessian curves $\mathrm{H}_{c,d}$ with $j(\mathrm{H}_{c,d}) = a$. So, $\#i_H(a)$ is the number of distinct generalized Hessian curves with j-invariant a that are twists of each other. Clearly, $\#i_H(a) = 0$, if $a \notin J_{\mathrm{H}}$. We note that, for all elliptic curve E over $\mathbb{F}_q$, we have $\#E(\mathbb{F}_q) + \#E_t(\mathbb{F}_q) = 2q+2$, where E_t is the nontrivial quadratic twist of E. We also recall that the order of the group of $\mathbb{F}_q$-rational points of a generalized Hessian curve is divisible by 3 (see Theorem 2). Since $q \equiv 1 \pmod 3$, if the isomorphism class of $\mathrm{H}_{c,d}$ is in $i_H(a)$ then the isomorphism class of the nontrivial quadratic twist of $\mathrm{H}_{c,d}$ is not in $i_H(a)$. So, $\#i_H(a) = 1$ if $a \in J_{\mathrm{H}}$ and $a \neq 0, 1728$. Moreover, one can show that $\#i_H(a) = 3$ if $a = 0$ and $\#i_H(a) = 1$ if $a = 1728$, $a \neq 0$ and $a \in J_{\mathrm{H}}$. Therefore, we have

$$I_{\mathrm{H}}(q) = \sum_{a \in \mathbb{F}_q} i_H(a) = \sum_{a \in J_{\mathrm{H}}} i_H(a) = 2 + \sum_{a \in J_{\mathrm{H}}} 1 = 2 + J_{\mathrm{H}}(q) \ .$$

From the proof of Theorem 4, we have

$$I_{\mathrm{H}}(q) = \begin{cases} (3q+9)/4, & \text{if } q \equiv 1 \pmod{12} \\ (3q+8)/4, & \text{if } q \equiv 4 \pmod{12} \\ (3q+7)/4, & \text{if } q \equiv 7 \pmod{12} \end{cases},$$

which completes the proof. □