Elliptic Curves in Generalized Huff's Model

Ronal Pranil Chand[1] and Maheswara Rao Valluri[2]
[1,2]School of Mathematical and Computing Sciences
Fiji National University
P.O.Box:7222, Derrick Campus, Suva, Fiji
{ronal.chand, maheswara.valluri}@fnu.ac.fj

Abstract

This paper introduces a new form of elliptic curves in generalized Huff's model. These curves endowed with the addition are shown to be a group over a finite field. We present formulae for point addition and doubling point on the curves, and evaluate the computational cost of point addition and doubling point using projective, Jacobian, Lopez-Dahab coordinate systems, and embedding of the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system. We also prove that the curves are birationally equivalent to Weierstrass form. We observe that the computational cost on the curves for point addition and doubling point is lowest by embedding the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system than the other mentioned coordinate systems and is nearly optimal to other known Huff's models.

Keywords: Doubling points, elliptic curves, groups, Huff's model, projective coordinates, scalar multiplication, birational forms.

MSC2010 (Mathematical Subject Classification): 11G05, 11G07, 14H52.

1 Introduction

Elliptic curves are algebraic curves and have been widely studied in number theory and cryptography [22, 18, 7, 17, 21]. The study of elliptic curves could be of various areas: Algebra, Algebraic Geometry, Number Theory, Diophantine problems, and so on. Lang [25] mentions in his book that

$$"It\, is\, possible\, to\, write\, endlessly\, on\, elliptic\, curves.\, (This\, is\, not\, a\, treat.)"$$

In 1995, Andrew Wiles proved the *Fermat's Last Theorem* using proof of the modularity conjecture for semistable elliptic curves [32]. The use of elliptic curves have commercialized and are studied extensively for its application in cryptography [15, 8, 9].

The plane curves of degree 3 are known as cubics and have the general form of

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0.$$

Elliptic curves are non-singular cubic curves and have points defined over a field $\mathbb{K}$ [14, 30].

In the mid-1980s, Koblitz and Miller independently proposed Elliptic Curve Cryptography (ECC) using the Elliptic Curve Discrete Logarithmic Problem (ECDLP) [23, 26]. The ECC provides better security when compared to Diffie-Hellman (DH) key exchange and Rivest-Shamir-Adleman (RSA) algorithm, but the underlying arithmetic group is more tedious, which makes the study particularly interesting for systems with confined computing power and memory [24].

Some of the famous forms of elliptic curves existing in literature are Weierstrass cubics [14, 30], Hessian curves [6, 21], Jacobi quartics [7], Montgomery [27], Edwards [4, 5, 13, 2, 11] and Huff's curve [18]. There has been a lot of development to these models of elliptic curves, for instance, Joye et al. studied Huff's model for elliptic curves in 2010 [22]. In 2012, Wu and Feng also carried out research on Huff's curves in [33]. A year later, Binary Huff's curves were investigated by Devigne and Joye [12]. In 2015, He et al. [17] studied generalized Huff's curves. The recent study on Huff's curves was done by Orhon and Hisil in [29]. The different families of Huff's elliptic curves studied over the past decade are listed below.

1. The curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Joye et al. in [22] are of the form of:
$$ax(y^2-1) = by(x^2-1), \text{where}\, a^2-b^2 \neq 0,$$

2. The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Joye et al. in [22] are of the form of:
$$ax(y^2-d) = by(x^2-d), \text{where}\, abd(a^2-b^2) \neq 0,$$

3. The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Wu and Feng in [33] are of the form of:
$$x(ay^2-1) = y(bx^2-1), \text{where}\, ab(a-b) \neq 0,$$

4. The binary Huff curves over a field $\mathbb{K}$, char($\mathbb{K}$) $= 2$ by Joye et al. in [12] are of the form of:
$$ax(y^2+y+1) = by(x^2+x+1), \text{where}\, ab(a-b) \neq 0,$$

5. The generalized binary Huff curves over a field $\mathbb{K}$, char($\mathbb{K}$) $= 2$ by Joye et al. in [22] are of the form of:
$$ax(y^2+fy+1) = by(x^2+fx+1), \text{where}\, abf(a-b) \neq 0,$$

6. The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Ciss and Sow in [10] are of the form of:
$$ax(y^2-c) = by(x^2-d), \text{where}\, abcd(a^2c-b^2d) \neq 0.$$

7. The generalized Huff's curves over finite field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Orhon and Hisil in [29] are of the form of:
$$y(1+ax^2) = cx(1+dy^2)\,\text{where,}\, acd(a-c^2d) \neq 0.$$

We can also find similar progress of other elliptic curves. For instance, after the introduction of Edwards curve in [13] by Harold Edwards, it became an active area of research resulting in an extensive literature [3, 4, 5, 19, 1, 2].

In this paper, we introduce a new form of elliptic curves in generalized Huff's model over a field $\mathbb{K}$, $\mathrm{char}(\mathbb{K}) \neq 2$ which are of the form

$$E(\mathbb{K}) : ax\left(y^2 + xy + f\right) = by\left(x^2 + xy + g\right),$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$. We show that the curves satisfy axioms of an abelian group under addition operation. Furthermore, we provide formulae for point addition and doubling point in affine, projective, Jacobian, Lopez-Dahab coordinates, embedding of the curve into $\mathbb{P}^1 \times \mathbb{P}^1$, and including an estimate of the number of points on E over a field $\mathbb{K}$. We also evaluate computational cost in each coordinate systems and compare computational cost with other known Huff's curves.

The rest of the paper is organized as follows. In section 2, we show that the introduced a new form elliptic curves in generalized Huff's model are commutative groups over a finite field; and give formulae for point addition and doubling points for affine, projective, Jacobian, and Lopez-Dahab coordinate systems. Furthermore, the next section is on embedding of Huff's model of elliptic curve into $\mathbb{P}^1 \times \mathbb{P}^1$ system and its computational cost. In section 4, we provide an estimate of the number of points on $E(\mathbb{K})$ with a toy example. We also show that the new form of Huff's curves are birationally equivalent to Weierstrass form in section 5. In section 6, we give computational cost analysis and comparison for the curves on different coordinate systems and other forms of Huff's curve in literature. Finally, we give conclusion remarks in Section 7.

2 Generalized Huff's Model

Let $\mathbb{K}$ be a finite field of characteristic $\neq 2$. We define an elliptic curve, denote it by E over $\mathbb{K}$ as

$$E(\mathbb{K}) : ax\left(y^2 + xy + f\right) = by\left(x^2 + xy + g\right), \tag{2.1}$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$. The $\jmath-invariant$ of E is given by $\frac{256\left(a^2f^2+abfg+b^2g^2\right)^3}{a^2b^2f^2g^2(af+bg)^2}$.The inflection point $(0, 0, 1)$ of $E(\mathbb{K})$ has the tangent line as $bgy = afx$, that passes through the curve with the multiplicity of 3, thus $O = (0 : 0 : 1)$ is a neutral point of $E(\mathbb{K})$. Furthermore, we denote group law as $\oplus$. Figure 2.1 shows that the line passing through the points P and Q, and intersecting at the third point R on $E(\mathbb{K})$.

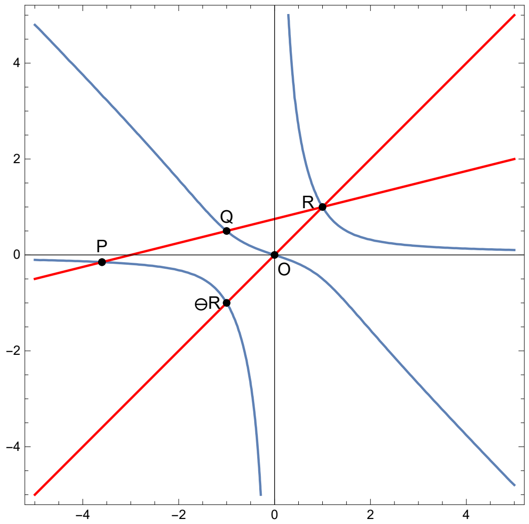

Figure 2.1: An example of the elliptic curve $E(\mathbb{K})$

Let $P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$ and $R = (X_3 : Y_3 : Z_3)$ be three points on $E(\mathbb{K})$. Then, $P \oplus Q$ could be obtained by the line connecting R and O that intersects at the third point $\ominus R$ on $E(\mathbb{K})$ such that $P \oplus Q = \ominus R$ which implies that $P \oplus Q \oplus R = O$. In particular, the inverse of the point P is $\ominus P = (X_1 : Y_1 : -Z_1)$. It is clear that the curve $E(\mathbb{K})$ posses commutative law. We note that there are three points at infinity, namely $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$ on $E(\mathbb{K})$, and the sum of any two points at infinity equals to the third point. For any point $(X_1 : Y_1 : Z_1)$, when $Z_1 \neq 0$, for some real number α and γ bounded by the field $\mathbb{K}$, we observe that

$$(1 : 0 : 0) \oplus (X_1 : Y_1 : Z_1) = (\alpha Z_1^2 : -X_1Y_1 : X_1Z_1) \text{ and}$$

$$(0 : 1 : 0) \oplus (X_1 : Y_1 : Z_1) = (-X_1Y_1 : \gamma Z_1^2 : Y_1Z_1).$$

Furthermore, we note that

$$(a : b : 0) \oplus (X_1 : Y_1 : Z_1) = (0 : 1 : 0) \oplus (\alpha Z_1^2 : -X_1Y_1 : X_1Z_1), \text{ therefore}$$

$$(a : b : 0) \oplus (X_1 : Y_1 : Z_1) = \begin{cases} (a : b : 0) \text{ if } (X_1 : Y_1 : Z_1) & = \quad (0 : 0 : 1) \\ (-\alpha Y_1Z_1 : -\gamma X_1Z_1 : X_1Y_1) & \quad \text{otherwise} \end{cases}.$$

We have doubling point if $P = Q$, thus the line connecting P and Q is the tangent at the point P.

2.1 Affine Formulae

This subsection provides explicit formulae for the group law for the elliptic curve defined by equation (2.1).

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, y_3)$ be the three different points on $E(\mathbb{K})$ such that R is obtained by connecting a line through P and Q. Let the secant line joining P and

Q has the slope defined as $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. Thus, $y = \lambda x + \beta$ is the equation of the secant line passing through the points P, Q and R, where $\beta = y_1 - \lambda x_1$. For the curve equation (2.1), we can replace y with $\lambda x + \beta$. Then,

$$\begin{aligned} ax((\lambda x+\beta)^2 + x(\lambda x+\beta) + f) =& b(\lambda x+\beta) \\ & (x^2 + x(\lambda x+\beta) + g).\text{This implies that} \\ x\left(af + a\beta^2\right) + x^2(a\beta + 2a\beta\lambda) & \\ +x^3\left(a\lambda + a\lambda^2\right) =& \left(bg\beta + x\left(b\beta^2 + bg\lambda\right)\right. \\ & + x^2(b\beta + 2b\beta\lambda) + x^3\left(b\lambda + b\lambda^2\right). \end{aligned} \tag{2.2}$$

Let

$$A = a\beta - b\beta + 2a\beta\lambda - 2b\beta\lambda$$

and

$$B = a\lambda - b\lambda + a\lambda^2 - b\lambda^2.$$

Then, equation (2.2) becomes

$$-bg\beta + x\left(af + a\beta^2 - b\beta^2 - bg\lambda\right) + Ax^2 + Bx^3 = 0 \tag{2.3}$$

.

We now note that

$$x_1 + x_2 + x_3 = -\frac{A}{B}, \tag{2.4}$$

$$-x_3 = x_1 + x_2 + \frac{a\beta - b\beta + 2a\beta\lambda - 2b\beta\lambda}{a\lambda - b\lambda + a\lambda^2 - b\lambda^2},$$

substituting $\beta = y_1 - \lambda x_1$ and $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

$$\begin{aligned} x_3 &= -\left(x_1 + x_2 + \frac{(x_1 - x_2 + 2y_1 - 2y_2)(-x_2y_1 + x_1y_2)}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)}\right) \\ &= -x_1 - x_2 - \frac{(x_1 - x_2 + 2y_1 - 2y_2)(-x_2y_1 + x_1y_2)}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)}, \end{aligned}$$

which simplifies to

$$x_3 = -\frac{(x_1 - x_2)(y_1(x_1 + y_1) - y_2(x_2 + y_2))}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)}. \tag{2.5}$$

We claim, by symmetry that

$$y_3 \quad = \quad -\frac{(y_1 - y_2)\left(x_1^2 + x_1 y_1 - x_2 (x_2 + y_2)\right)}{(x_1 - x_2)(x_1 - x_2 + y_1 - y_2)}. \tag{2.6}$$

Thus, this is an evidence that the curve $E(\mathbb{K})$ has three points $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, y_3)$. We observe that inverse of the point R is $\ominus R = (-x_3, -y_3)$. We note that the point $R = (x_3, y_3)$ is computed only when $x_1 \neq x_2$, $y_1 \neq y_2$ and $x_1 - x_2 + y_1 - y_2 \neq 0$ and the addition formula used in the affine coordinate system could not be employed for doubling points since $x_1 \neq x_2$ and $y_1 \neq y_2$.

Theorem 1. *Let $E(\mathbb{K})$ be a elliptic curve defined by equation (2.1) with $abfg(a - b) \neq 0$ and points P, Q and $\mathcal{O} = (0, 0)$ on $E(\mathbb{K})$. $\mathcal{O}$ is a neutral point. Then E has the following properties:*

1. *If $P = \mathcal{O}$, then $P \oplus Q = Q$.*
2. *Otherwise, if $Q = \mathcal{O}$, then $P \oplus Q = P$.*
3. *Otherwise, let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.*
4. *If $-x_1 = x_2$ and $-y_1 = y_2$, then $P \oplus Q = \mathcal{O}$.*
5. *Otherwise, let*

   $x_3 = -\frac{(x_1 - x_2)(y_1(x_1 + y_1) - y_2(x_2 + y_2))}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)}$ *and* $y_3 = -\frac{(y_1 - y_2)\left(x_1^2 + x_1 y_1 - x_2(x_2 + y_2)\right)}{(x_1 - x_2)(x_1 - x_2 + y_1 - y_2)}$.

   Then $P \oplus Q = (-x_3, -y_3)$

Proof. Parts (1) and (2) are a similar concept and is easy to see. For (1), P is the neutral point (0,0), then the line through P and Q intersects E with the of 3, as P, Q and $-Q$. To obtain $P \oplus Q$, one must take the inverse of the third point of the intersection. Thus, $-(-Q) = Q$. The similar proof follows for (2). Part (4) is also easily obtained. If $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (-x_1, y_1)$ then the third point of intersection of P and Q is $\mathcal{O}$. The inverse of $\mathcal{O}$ is $-\mathcal{O} = \mathcal{O}$. To prove (5), we take the algebraic step. We note that if points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two distinct points on E and neither of them equivalent to $\mathcal{O}$, then the line through points P and Q has the slope as λ. The line equation could be written as $y = \lambda x + \beta$, where $\beta = y_1 - \lambda x_1$. Substituting the line equation in $E(\mathbb{K})$ gives us the equation (2.3). It is clear that x_1 and x_2 are two roots of the above cubic equation; thus, we can write,

$$\begin{aligned}(x - x_1)(x - x_2)(x - x_3) = x^3 &+ (-x_1 - x_2 - x_3)x^2 \\ &+ (xx_2 + x_3 x_2 + x_1 x_3)x - x_1 x_2 x_3.\end{aligned}$$

Then the proof follows the derivation of equation (2.5) and equation (2.6). □

We now define a point of infinity on $E(\mathbb{K})$ as $\mathcal{O} = (0,0)$. For the point $P = (x_1, y_1)$, we have $\ominus P = (-x_1, -y_1)$. Thus, it follows that

$$\begin{aligned}
x_3 &= -\frac{(x_1 - x_2)(y_1(x_1 + y_1) - y_2(x_2 + y_2))}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)} \\
&= -\frac{(x_1 - -x_1)(y_1(x_1 + y_1) - -y_2(-x_2 - y_2))}{(y_1 - -y_2)(x_1 - -x_2 + y_1 - -y_2)} \\
&= -\frac{(x_1 + x_1)(y_1(x_1 + y_1) + y_1(-x_1 - y_1))}{(y_1 - -y_1)(x_1 - -x_1 + y_1 - -y_1)} \\
&= -\frac{(2x_1)(0)}{(2y_1)(2x_1 + 2y_1)} \\
&= 0,
\end{aligned}$$

and

$$\begin{aligned}
y_3 &= -\frac{(y_1 - y_2)(x_1^2 + x_1y_1 - x_2(x_2 + y_2))}{(x_1 - x_2)(x_1 - x_2 + y_1 - y_2)} \\
&= -\frac{(y_1 - -y_1)(x_1^2 + x_1y_1 - -x_1(-x_1 - y_1))}{(x_1 - -x_1)(x_1 - -x_1 + y_1 - -y_1)} \\
&= -\frac{(2y_1)(x_1^2 + x_1y_1 + x_1(-x_1 - y_1))}{(x_1 + x_1)(x_1 + x_1 + y_1 + y_1)} \\
&= -\frac{(2y_1)(0)}{(2x_1)(2x_1 + 2y_1)} \\
&= 0.
\end{aligned}$$

Thus $P \oplus (\ominus P) = \mathcal{O}$.

Corollary 2. *The identity $\mathcal{O}$ is always on the elliptic curve defined by*

$$E:\ ax(y^2 + xy + f) = by(y^2 + xy + g)$$

where $abfg(a - b) \neq 0$.

Theorem 3. *A line cutting $E(\mathbb{K})$ at three distinct points namely P,Q and R. The associative law on these points is equivalent to $\mathcal{O} = (0,0)$.*

Proof. We now show that the curve $E(\mathbb{K})$ holds associative law, that is $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.
For x-coordinates,
we have

$$Q \oplus R = \frac{(x_2 - x_3)(y_2(x_3 + y_2) - y_3(x_3 + y_3))}{(y_2 - y_3)(x_2 - x_3 + y_2 - y_3)}$$

and by equation (2.5),

$$P = \frac{(x_2 - x_3)\left(y_2\left(x_3 + y_2\right) - y_3\left(x_3 + y_3\right)\right)}{(y_2 - y_3)\left(x_2 - x_3 + y_2 - y_3\right)}$$

then

$$\begin{aligned}
P \oplus (Q \oplus R) &= -\frac{(x_2 - x_3)\left(y_2\left(x_3 + y_2\right) - y_3\left(x_3 + y_3\right)\right)}{(y_2 - y_3)\left(x_2 - x_3 + y_2 - y_3\right)} + \\
&\quad \frac{(x_2 - x_3)\left(y_2\left(x_3 + y_2\right) - y_3\left(x_3 + y_3\right)\right)}{(y_2 - y_3)\left(x_2 - x_3 + y_2 - y_3\right)}. \\
&= 0
\end{aligned}$$

It follows that,

$$\begin{aligned}
(P \oplus Q) \oplus R &= -\frac{(x_1 - x_2)\left(y_1\left(x_1 + y_1\right) - y_2\left(x_2 + y_2\right)\right)}{(y_1 - y_2)\left(x_1 - x_2 + y_1 - y_2\right)} + \\
&\quad \frac{(x_1 - x_2)\left(y_1\left(x_1 + y_1\right) - y_2\left(x_2 + y_2\right)\right)}{(y_1 - y_2)\left(x_1 - x_2 + y_1 - y_2\right)} \\
&= 0
\end{aligned}$$

For y-coordinates, we have

$$\begin{aligned}
P \oplus (Q \oplus R) &= -\frac{(y_2 - y_3)\left(x_2^2 + x_2 y_2 - x_3\left(x_3 + y_3\right)\right)}{(x_2 - x_3)\left(x_2 - x_3 + y_2 - y_3\right)} \\
&\quad +\frac{(y_2 - y_3)\left(x_2^2 + x_2 y_2 - x_3\left(x_3 + y_3\right)\right)}{(x_2 - x_3)\left(x_2 - x_3 + y_2 - y_3\right)}. \\
&= 0
\end{aligned}$$

and

$$\begin{aligned}
(P \oplus Q) \oplus R &= -\frac{(y_1 - y_2)\left(x_1^2 + x_1 y_1 - x_2\left(x_2 + y_2\right)\right)}{(x_1 - x_2)\left(x_1 - x_2 + y_1 - y_2\right)} + \\
&\quad \frac{(y_1 - y_2)\left(x_1^2 + x_1 y_1 - x_2\left(x_2 + y_2\right)\right)}{(x_1 - x_2)\left(x_1 - x_2 + y_1 - y_2\right)} \\
&= 0
\end{aligned}$$

In both scenario we get $\mathcal{O}$. Now to get final point we must reflect $\mathcal{O}$ on $\mathcal{O}$ (that is, $\mathcal{O} \oplus \mathcal{O}$), however $\mathcal{O}$ is the neutral point thus, we have

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

□

2.2 Doubling Point

The slope of the tangent line on the curve defined by equation (2.1), could be computed by implicit differentiation, thus by differentiation of $E(\mathbb{K})$ with respect to x, we have

$$\begin{aligned} af + 2axy + ay^2 + ax^2y' + 2axyy' &= 2bxy + by^2 + bgy' + bx^2y' + 2bxyy' \\ y' &= \frac{af + 2axy + ay^2 - 2bxy - by^2}{bg - ax^2 + bx^2 - 2axy + 2bxy}. \end{aligned}$$

For the point $P = (x_1, y_1)$, we can describe the slope as

$$\lambda_p = \frac{af + 2ax_1y_1 + ay_1^2 - 2bx_1y_1 - by_1^2}{bg - ax_1^2 + bx_1^2 - 2ax_1y_1 + 2bx_1y_1} = \frac{af + (a-b)y_1\,(2x_1 + y_1)}{bg - (a-b)x_1\,(x_1 + 2y_1)}.$$

Let

$$A_1 = afx_1 + (2af + bg + (a-b)x_1^2)\,y_1,\ A_2 = 3(a-b)x_1y_1^2 + 2(a-b)y_1^3, \\ A_3 = (bg - (a-b)x_1\,(x_1 + 2y_1))$$

and

$$B_1 = (af + (a-b)y_1\,(2x_1 + y_1)),\ B_2 = 2(-a+b)x_1^3 + bgy_1 + 3(-a+b)x_1^2y_1, \\ B_3 = x_1\,(af + 2bg + (-a+b)y_1^2).$$

We claim that

$$x_2 = -\frac{A_3\,(A_1 + A_2)}{(af + bg + (-a+b)x_1^2 + (a-b)y_1^2)\,(af + (a-b)y_1\,(2x_1 + y_1))} \tag{2.7}$$

and

$$y_2 = -\frac{B_1\,(B_2 + B_3)}{(af + bg + (-a+b)x_1^2 + (a-b)y_1^2)\,(bg - (a-b)x_1\,(x_1 + 2y_1))} \tag{2.8}$$

are the second coordinates of the point of intersection for the tangent line at P. We can prove our claim by simply checking the slope given by

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

and by simplification, we can obtain

$$\lambda = \frac{af + (a-b)y_1\,(2x_1 + y_1)}{bg - (a-b)x_1\,(x_1 + 2y_1)}$$

which have the same slope as λ_p.

2.3 Projective formulae

Let $x = \dfrac{X}{Z}$, $y = \dfrac{Y}{Z}$ and $Z = 1$ [14, 30], then the affine coordinate of equation (2.1) becomes,

$$a\frac{X}{Z}\left(\frac{Y^2}{Z^2} + \frac{XY}{Z^2} + f\right) \quad = \quad b\frac{Y}{Z}\left(\frac{X^2}{Z^2} + \frac{XY}{Z^2} + g\right).$$

Finally, multiplying by Z^3 on both the sides to get rid of denominators and achieve the projective form of the curve equation

$$E(\mathbb{K}) : aX\left(Y^2 + XY + fZ^2\right) = bY\left(X^2 + XY + gZ^2\right), \tag{2.9}$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the point $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follows:

$$\begin{aligned} U_3 =& (X_2Z_1 - X_1Z_2)^2(Y_2Z_1^2(X_2 + Y_2) - Y_1Z_2^2(X_1 + Y_1)) \\ V_3 =& (Y_2Z_1 - Y_1Z_2)^2(X_2Z_1^2(X_2 + Y_2) - X_1Z_2^2(X_1 + Y_1)) \\ W_3 =& -Z_1Z_2(X_2Z_1 - X_1Z_2)(Y_2Z_1 - Y_1Z_2)(Z_1(X_2 + Y_2) - Z_2(X + Y_1)). \end{aligned} \tag{2.10}$$

For doubling points, the coordinates are as follows:

$$\begin{aligned} U_2 &= -(X_1(a-b)(X + 2Y_1) - bgZ_1^2)^2 \\ &\quad (Y_1(a-b)(X_1 + Y_1)(X_1 + 2Y_1) + Z_1^2(afX_1 + (2af + bg)Y_1)) \\ V_2 &= -(Y_1(a-b)(2X_1 + Y_1) + afZ_1^2)^2 \\ &\quad (-X_1(a-b)(X_1 + Y_1)(2X_1 + Y_1) + Z_1^2(X_1(af + 2bg) + bgX_1)) \\ W_2 &= Z_1(Y_1(a-b)(2X_1 + Y_1) + afZ_1^2)(-X_1(a-b)(X_1 + 2Y_1) + bgZ_1^2) \\ &\quad (-(a-b)(X_1^2 - Y_1^2) + (af + bg)Z_1^2). \end{aligned} \tag{2.11}$$

Theorem 4. *Let $\mathbb{K}$ be a finite field of characteristic $\neq 2$. Let $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$ be two points on $E(\mathbb{K})$. Then, the addition formula given by equation 2.10 is valid provided that $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$ and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$.*

Proof. Let P_1 and P_2 be finite points, we can write $P_1 = (x_1, y_1)$, and $P_2 = (x_2, y_2)$, where $(x_1, y_1) \neq (0, 0)$ and $(x_2, y_2) \neq (0, 0)$. The point addition given by the equations (4.5) and (4.6) is only valid if $x_1 \neq x_2$, $y_1 \neq y_2$ and $x_1 - x_2 + y_1 - y_2 \neq 0$, which translate to projective coordinates as $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$ and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$, respectively.

It remains to analyze that the condition is satisfied at the infinity points. The points at infinity are $(1:0:0)$, $(0:1:0)$ and $(a, b, 0)$, if P_1 or $P_2 \in \{(1:0:0), (0:1:0)\}$, then $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$ and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$ is not satisfied. Since $P_1 \notin \{O, (1:0:0), (0:1:0)\}$ then the addition law is valid for $P_2 = (a:b:0)$ as mentioned earlier. □

2.3.1 Computational cost analysis on Projective Coordinates

We evaluate the efficiency of point addition and doubling point on the curve $E(\mathbb{K})$. The computation cost ratio between a square (s) and multiplication (m) is typically $s = 0.8m$. We omit other operations such as (a) and (d) as computation cost is lower.

Projective coordinates may be preferred for faster arithmetic than the affine formula. The affine formulae are given by equation (2.5) and (2.6) for the addition of two different points on $E(\mathbb{K})$ is described by equation (2.10).

We let the cost of a multiplication be m and the cost of a square be s in the field $\mathbb{K}$. Then, we have

$$m_1 = X_1Z_2,\ m_2 = X_2Z_1,\ m_3 = Y_1Z_2,\ m_4 = Y_2Z_1,$$

$$m_5 = m_4(m_2 + m_4),\ m_6 = m_3(m_1 + m_3),\ m_7 = m_2(m_2 + m_4),\ m_8 = m_1(m_1 + m_3),$$
$$m_9 = -Z_1Z_2,$$

$$s_1 = (m_2 - m_1)^2,\ s_2 = (m_4 - m_3)^2,$$

$$U_3 = s_1(m_5 - m_6),\ V_3 = s_2(m_7 - m_8),\ W_3 = m_9(m_2 - m_1)(m_4 - m_3)(m_2 + m_4 - m_1 - m_3).$$

Therefore, the total cost of point addition on the curve $E(\mathbb{K})$ is $14m + 2s$.

For the doubling point as described by equation (2.11), we have

$$s_1 = Z_1^2,\ s_2 = X_1^2,\ s_3 = Y_1^2,$$

$$m_1 = X_1(a - b)(X_1 + 2Y_1),\ m_2 = (X_1 + Y_1)(X_1 + 2Y_1),\ m_3 = s_1(afX_1 + Y_1(2af + bg)),$$
$$m_4 = (a - b)Y_1m_2,\ m_5 = Y_1(a - b)(2X_1 + Y_1)$$

$$m_6 = (X_1 + Y_1)(2X_1 + Y_1),\ m_7 = s_1((af + 2bg)X_1 + bgY_1),\ m_8 = -X_1m_6(a - b),$$
$$m_9 = (m_5 + afs_1)((a - b)(s_2 + s_3) + s_1(af + bg))$$

$$U_2 = -(m_1 - bgs_1)^2(m_3 + m_4),\ V_2 = -(m_5 + afs_1)^2(m_7 + m_8),\ W_2 = -m_1m_9Z_1.$$

Therefore, the total cost of doubling point on the curve $E(\mathbb{K})$ is $13m + 5s$.

2.4 Jacobian formulae

Let $x = \dfrac{X}{Z^2}$, $y = \dfrac{Y}{Z^3}$ and $Z = 1$ [14, 30]. Then the affine coordinate given by equation (2.1) after simplification becomes,

$$E(\mathbb{K}) :\ aX(Y^2 + XYZ + fZ^6) = bY(XZ^2 + XYZ + gZ^6),$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a - b) \neq 0$.

For the point $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follows:

$$\begin{aligned}
U_3 &= -Z_1Z_2\left(X_2Z_1^2 - X_1Z_2^2\right)^2\left(Y_2^2Z_1^6 + X_2Y_2Z_1^6Z_2 - Y_1Z_2^6\left(Y_1 + X_1Z_1\right)\right),\\
V_3 &= -\left(Y_2Z_1^3 - Y_1Z_2^3\right)^2\left(X_2Y_2Z_1^5 + X_2^2Z_1^5Z_2 - X_1Z_2^5\left(Y_1 + X_1Z_1\right)\right),\\
W_3 &= Z_1^2Z_2^2\left(Y_2Z_1^3 - Y_1Z_2^3\right)\left(X_2Z_1^3Z_2 - X_1Z_1Z_2^3\right)\left(Y_2Z_1^3 + X_2Z_1^3Z_2 - Z_2^3\left(Y_1 + X_1Z_1\right)\right).
\end{aligned}$$

For doubling points, the coordinates are as follows:

$$\begin{aligned}
U_2 &= -Z_1\left(2X_1Y_1(-a+b) + (-a+b)X_1^2Z_1 + bgZ_1^5\right)^2\\
&\quad \left(2(a-b)Y_1^3 + 3(a-b)X_1Y_1^2Z_1 + afX_1Z_1^7 + Y_1Z_1^2\left((a-b)X_1^2 + (2af+bg)Z_1^4\right)\right),\\
V_2 &= -\left((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^6\right)^2\\
&\quad \left(3(-a+b)X_1^2Y_1Z_1 + 2(-a+b)X_1^3Z_1^2 + bgY_1Z_1^5 + X_1\left((-a+b)Y_1^2 + (af+2bg)Z_1^6\right)\right),\\
W_2 &= Z_1^3\left(2(-a+b)X_1Y_1 + (-a+b)X_1^2Z_1 + bgZ_1^5\right)\left((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^6\right)\\
&\quad \left((a-b)Y_1^2 + (-a+b)X_1^2Z_1^2 + (af+bg)Z_1^6\right).
\end{aligned}$$

The costs of point addition and doubling point on the curve $E(\mathbb{K})$ are $32m{+}4s$ and $29m{+}5s$, respectively.

2.5 Lopez-Dahab formuale

Let $x = \dfrac{X}{Z}$, $y = \dfrac{Y}{Z^2}$ and $Z = 1$ [14, 30]. Then the affine coordinate given by equation (2.1) after simplification becomes,

$$E(\mathbb{K}):\ aX(Y^2 + XYZ + fZ^5) = bY(XZ^2 + XY + gZ^6),$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the point $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follows:

$$\begin{aligned}
U_3 &= -Z_1Z_2\left(X_2Z_1 - X_1Z_2\right)^2\left(Y_2^2Z_1^4 + X_2Y_2Z_1^4Z_2 - Y_1Z_2^4\left(Y_1 + X_1Z_1\right)\right),\\
V_3 &= -\left(Y_2Z_1^2 - Y_1Z_2^2\right)^2\left(X_2Y_2Z_1^3 + X_2^2Z_1^3Z_2 - X_1Z_2^3\left(Y_1 + X_1Z_1\right)\right),\\
W_3 &= Z_1^2Z_2^2\left(X_2Z_1 - X_1Z_2\right)\left(Y_2Z_1^2 - Y_1Z_2^2\right)\left(Y_2Z_1^2 + Z_2\left(X_2Z_1^2 - Z_2\left(Y_1 + X_1Z_1\right)\right)\right).
\end{aligned}$$

For doubling points, the coordinates are as follows:

$$\begin{aligned}
U_2 &= -Z_1\left(2(-a+b)X_1Y_1 + (-a+b)X_1^2Z_1 + bgZ_1^3\right)^2\\
&\quad \left(2(a-b)Y_1^3 + 3(a-b)X_1Y_1^2Z_1 + afX_1Z_1^5 + Y_1Z_1^2\left((a-b)X_1^2 + (2af+bg)Z_1^2\right)\right),\\
V_2 &= -\left((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^4\right)^2\\
&\quad \left(3(-a+b)X_1^2Y_1Z_1 + 2(-a+b)X_1^3Z_1^2 + bgY_1Z_1^3 + X_1\left((-a+b)Y_1^2 + (af+2bg)Z_1^4\right)\right),\\
W_2 &= Z_1^2\left(2(-a+b)X_1Y_1 + (-a+b)X_1^2Z_1 + bgZ_1^3\right)\left((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^4\right)\\
&\quad \left((a-b)Y_1^2 + (-a+b)X_1^2Y_1^2 + (af+bg)Z_1^4\right).
\end{aligned}$$

The costs of point addition and doubling point on the curve $E(\mathbb{K})$ are $32m{+}6s$ and $26m{+}5s$, respectively.

3 Embedding of Huff's Model of Elliptic Curves into $\mathbb{P}^1 \times \mathbb{P}^1$

It is noted that computational cost is higher while using projective, Jocobian or Lopez-Dahab. Thus changing the form of the curve could yield a better result.

Theorem 5. *The elliptic curve $E(\mathbb{K}) : ax(y^2 + xy + f = by(x^2 + xy + g)$ could be written has $E(\mathbb{K}) : x(y^2 - c) = y(x^2 - d)$ where $c = \dfrac{-af}{a-b}$ and $d = \dfrac{bg}{a-b}$.*

Proof. We have $E(\mathbb{K}) : ax(y^2 + xy + f = by(x^2 + xy + g)$ has

$$\begin{aligned} axy^2 + ax^2y + afx - bx^2y - bxy^2 - bgy &= 0, \\ axy^2 - bxy^2 + afx + ax^2y - bxy^2 - bgy &= 0, \\ x(ay^2 - by^2 + af) + y(ax^2 - bx^2 - bg) &= 0, \\ x((a-b)y^2 + af) - y(-x^2(a-b) + bg) &= 0, \end{aligned}$$

finally, we can scale the equations by $a - b$ since $a - b \neq 0$. We obtain $E(\mathbb{K})$ of the following forms,

$$\begin{aligned} \frac{x((a-b)y^2 + af)}{a-b} - \frac{y(-x^2(a-b) + bg)}{a-b} &= 0 \\ x\left(y^2 + \frac{af}{a-b}\right) - y\left(-x^2 + \frac{bg}{a-b}\right) &= 0. \end{aligned}$$

Let $c = \dfrac{-af}{a-b}$ and $d = \dfrac{bg}{a-b}$ then we can simplify the equation as follows,

$$\begin{aligned} xy^2 - cx - yx^2 + yd = 0 \\ E(\mathbb{K}) :\ x(y^2 - c) = y(x^2 - d). \end{aligned}$$

□

We note that the elliptic curve given by $E(\mathbb{K}) :\ ax(y^2 - c) = by(x^2 - d)$ is a generalized Huff's elliptic curve by Ciss and Sow [10].

3.1 Efficiency of Elliptic curve $E(\mathbb{K}) : x(y^2 - c) = y(x^2 - d)$

According to Ciss and Sow [10], their model of Huff's elliptic curve is

$$E(\mathbb{K}) : ax(y^2 - c) = by(x^2 - d) \tag{3.1}$$

where $abcd(a^2c - b^2d) \neq 0$. We can see that the proposed curve given by equation (3.1) has unified formulas for point addition and doubling point. The model by Ciss and Sow has unified formulas for point addition and doubling point. According to Ciss and Sow [10], the point addition on the curve is given by equation (3.2) and the doubling point is given by equation (3.3).

$$(x_1, y_1) + (x_2, y_2) = \begin{cases} x_3 = \dfrac{d(x_1 + x_2)(c + y_1y_2)}{(d + x_1x_2)(c - y_1y_2)}, \\ y_3 = \dfrac{c(y_1 + y_2)(d + x_1x_2)}{(c + y_1y_2)(d - x_1x_2)}. \end{cases} \tag{3.2}$$

$$[2](x_1, y_1) = \begin{cases} x_3 = \dfrac{2dx_1(c + y_1^2)}{(d + x_1^2)(c - y_1^2)}, \\ y_3 = \dfrac{2cy_1(d + x_1^2)}{(c + y_1^2)(d - x_1^2)}. \end{cases} \tag{3.3}$$

As shown by Ciss and Sow in [10] the total cost of point addition and doubling point is 12m+4d and 7m+5s+4d. The same results will be there for the proposed curve since point addition, and doubling point formulas do not include curve constant $'a'$ and $'b'$.

3.2 Embedding of $E(\mathbb{K}) : ax(y^2 - c) = by(x^2 - d)$ into $\mathbb{P}^1 \times \mathbb{P}^1$

The projective closure of elliptic curve defined by equation (3.1) in $\mathbb{P}^1 \times \mathbb{P}^1$ is given by

$$E(\mathbb{K}) = \{(X : Z), (Y : T) \in \mathbb{P}^1 \times \mathbb{P}^1 : aXZ(Y^2 - cT^2) = bTY(X^2 - dZ^2)\}. \tag{3.4}$$

The formula for point addition and doubling point then corresponds to the following:

$$((X_1 : Z_1), (Y_1 : T_1)) + ((X_2 : Z), (Y_2 : T_2)) =$$

$$\begin{aligned} &\{(d(XZ_1 + X_1Z_2)(cT_1T_2 + Y_1Y_2) : (cT_1T_2 - Y_1Y_2)(dZ_1Z_2 + X_1X_2)), \\ &(c(T_2Y_1 + T_1Y_2)(dZ_1Z_2 + X_1X_2) : (cT_1T_2 + Y_1Y_2)(X_1X_2 - dZ_1Z_2))\}. \end{aligned} \tag{3.5}$$

$$[2]((X_1 : Z_1), (Y_1 : T_1)) =$$

$$\begin{aligned} &\{(2dX_1Z_1(cT_1^2 + Y_1^2) : (cT_1^2 - Y_1^2)(dZ_1^2 + X_1^2)), \\ &(2cT_1Y_1(dZ_1^2 + X_1^2) : -(cT_1^2 + Y_1^2)(X_1^2 - dZ_1^2))\}. \end{aligned} \tag{3.6}$$

Cost for Point Addition

$$m_1 = X_1X_2,\ m_2 = dZ_1Z_2,\ m_3 = cT_1T_2,\ m_4 = Y_1Y_2,$$
$$m_5 = T_1Y_2,\ m_6 = X_2Z_1,\ m_7 = X_1Z_2,\ m_8 = T_2Y_1.$$

$$
\begin{aligned}
X_3 &= d(XZ_1 + X_1Z_2)(cT_1T_2 + Y_1Y_2) = d(m_3 + m_4)(m_6 + m_7) \\
Z_3 &= cT_1T_2 - Y_1Y_2)(dZ_1Z_2 + X_1X_2) = (m_3 - m_4)(m_1 + m_2) \\
Y_3 &= c(T_2Y_1 + T_1Y_2)(dZ_1Z_2 + X_1X_2) = c(m_8 - m_5)(m_6 + m_7) \\
T_3 &= cT_1T_2 + Y_1Y_2)(X_1X_2 - dZ_1Z_2) = -(m_3 + m_4)(m_1 - m_2) \qquad (3.7)
\end{aligned}
$$

The total cost is $12m + 6a + 4d$ which is same as using projective coordinates .
Cost for Doubling Point

$$s_1 = X_1^2,\ s_2 = Y_1^2,\ s_3 = T_1^2,\ s_4 = Z_1^2$$

$$
\begin{aligned}
X_3 &= 2dX_1Z_1(cT_1^2 + Y_1^2) = 2dX_1Z_1(cs_3 + s_2) \\
Z_3 &= (cT_1^2 - Y_1^2)(dZ_1^2 + X_1^2) = (cs_3 - s_2)(s_1 + ds_4) \\
Y_3 &= 2cT_1Y_1(dZ_1^2 + X_1^2) = 2cT_1Y_1(s_1 + ds_4) \\
T_3 &= -(cT_1^2 + Y_1^2)(X_1^2 - dZ_1^2) = -(cs_3 + s_2)(s_1 - ds_4) \qquad (3.8)
\end{aligned}
$$

The total cost comes to $6m + 4s + 4a + 4d$, which is less than the cost given by Ciss and Sow and projective coordinates on by equation (3.4). Using embedding of $E(\mathbb{K}) : ax(y^2 - c) = by(x^2 - d)$ into $\mathbb{P}^1 \times \mathbb{P}^1$ and $c = \dfrac{-af}{a-b}$ and $d = \dfrac{bg}{a-b}$ have improved the proposed elliptic curves computational cost. One can notice that the curve described by Ciss and Sow has higher cost when computing $2P$ then found by embedding $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$.

4 Rational Points on $E(\mathbb{K})$

We define a new form of Huff's model of elliptic curves

$$E(\mathbb{F}_q) : ax\left(y^2 + xy + f\right) = by\left(x^2 + xy + g\right), \qquad (4.1)$$

where $a, b, f, g \in \mathbb{F}_q$ and $abfg(a - b) \neq 0$ by replacing the field $\mathbb{K}$ by $\mathbb{F}_q$, where q is a prime in the equation (2.1). We observe that for each x, the curve (4.1) yields at most two values for y; and the point of infinity $(0, 0)$ is always on the curve $E(\mathbb{F}_q)$. Thus, we can set up an upper bound for the number of rationals on $E(\mathbb{F}_q)$ as

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

However, computing the exact number of points on the curve $E(\mathbb{F}_q)$ is a challenge to us. However, Hasse's theorem [16] on elliptic curve $E(\mathbb{F}_q)$ provides an estimate for the number of rational points over a finite field $\mathbb{F}_q$ as

$$| \#E(\mathbb{F}_q) - (q+1) | \leq 2\sqrt{q}.$$

For the understanding purpose, we discuss the following method:

The curve (4.1) can be written be as

$$E(\mathbb{F}_q) : afx + \left(-bg + ax^2 - bx^2\right) y + (ax - bx)y^2 = 0. \tag{4.2}$$

This may be seen as a quadratic equation in y. The discriminant of (4.2) can be calculated by

$$\Delta = -4afx(ax - bx) + \left(-bg + ax^2 - bx^2\right)^2 \tag{4.3}$$

and y can be rational if and only if $\Delta = r^2$ for some rational r. In this senario, we can easily find some points on the curve (4.1) by simply assigning values of a, f and g and solving for b. The following toy example shows how one can obtain y coordinates and compute point addition and doubling point.

Example 6. Let $q = 11$. We then put $a = 1$, $f = 1$, $x = 1$ and $g = -1$ in the curve equation (4.1). Then the discriminant of (4.1) becomes

$$\begin{aligned} r^2 &= -4a(ax - bx) + (-bg + ax^2 - bx^2)^2, \\ r^2 &= -4(1 - b) + 1, \\ r^2 &= 4b - 3. \end{aligned} \tag{4.4}$$

We note that $4b - 3$ must be a rational square to obtain rational points on the elliptic curve. When $r = 1$,the equation (4.4) gives $b = 1$ but we omit this value due to the initial condition, $abfg(a - b) \neq 0$ of the elliptic curve $E(\mathbb{F}_{11})$. When $r = 2$, the equation (4.4) gives $b = 3$. Now the curve equation (4.1) becomes $E(\mathbb{F}_{11}) : x\left(y^2 + xy + 1\right) = 3y\left(x^2 + xy - 1\right)$. It is easy to check that

$$\begin{aligned} E(\mathbb{F}_{11}) = &\{\mathcal{O}, (0,1), (1,0), (1,1), (1,5), (3,7), (4,1), (4,5), (5,7), (6,4), \\ &(7,6), (7,10), (8,4), (10,1), (10,6), (10,10)\}, \end{aligned}$$

so, $\#E(\mathbb{F}_{11}) = 16$. Since $P = (1,1) \in E(\mathbb{F}_{11})$ and $Q = (10,10) \in E(\mathbb{F}_{11})$, one can easily compute doubling point $2P = (8,4)$ and $2Q =(3,7)$ and point addition of the point $P + 2Q = (10,6)$ and $2P + Q = (1,5)$ on the curve $E(\mathbb{F}_{11})$ by using the equations (2.5), (2.6), (2.7) and (2.8).

Lemma 7. *If (x, y) is a rational point on*

$$E(\mathbb{K}) : ax\left(y^2 + xy + f\right) - by\left(x^2 + xy + g\right) = 0$$

and $x \neq 0$, $y \neq 0$, then $(-x, -y)$ is also rational point on $E(\mathbb{K})$.

Proof. It is clear that if (x, y) is rational, then $(-x, -y)$ also rational. All we have to do is to show that $(-x, -y)$ is also on $E(\mathbb{K})$. Substituting $(-x, -y)$ in $E(\mathbb{K})$ gives the following,

$$\begin{aligned} a(-x)\left((-y)^2 + (-x)(-y) + f\right) - b(-y)\left((-x)^2 + (-x)(-y) + g\right) &= 0, \\ -ax\left(y^2 + xy + f\right) + by\left(x^2 + xy + g\right) &= 0, \\ E(\mathbb{K}) :\ ax\left(y^2 + xy + f\right) - by\left(x^2 + xy + g\right) &= 0. \end{aligned}$$

Thus, $(-x, -y)$ is also rational point on $E(\mathbb{K})$. □

5 Birational Equivalence of the New Form of Huff's Curve to Weierstrass Form.

In 1928, Nagell proposed a simpler procedure to construct birational equivalence in the specific case of plane curves. Nagell's method failed in even characteristics. In [31], the author describes how Nagell's method [28] could be modified to suit any characteristics. One can visit chapter 8 of [20] for the details of Nagell's algorithm. This section shows how to acheive birational equivalence of the elliptic curve described by equation (2.1) to Weierstrass curves.

Theorem 8. *Let $E(\mathbb{K})$ be a non-singular elliptic curve defined by the affine formulae defined by equation* (2.1)*. $E(\mathbb{K})$ is birational equivalence to a Weierstrass form of*

$$y^2 = t^3 + a_2t^2 + a_4t + a_6,$$

where $t = x - \frac{A}{BC}$, $A = a(a-b)f(af+bg)$,$B = (a-b)bg(2af+bg)$,*and* $C = b^3g^3$.

Proof. It is easy to see that equation (2.1) is also equivalent to

$$axy^2 + ax^2y + axf = bx^2y + bxy^2 + byg.$$

The signs of a, b, f, and g are either positive or negative and never equal to zero. The curve has $O = (0, 0)$ as the point of inflection. The curve has $(0 : 1 : 0)$, the point at infinity in projective transformation. For simplicity, we take $E(\mathbb{K})$ in the following form:

$$E(\mathbb{K}) : (a-b)XY^2 + (a-b)X^2Y + afXZ^2 - bgYZ^2 = 0.$$

In chapter 8 [20], Cassels states that an elliptic curve genus 1 with at least a rational point on the curve and Weierstrass form is enough to get the birational equivalence to curve and where $\mathcal{O}$ is a rational point on the Weierstrass curve. If the curve has an inflectional tangent at point O, then let $\mathcal{O} = (0 : 1 : 0)$. The linear transformation of co-ordinates is enough to take O to $\mathcal{O}$ and the tangent the line at infinity. We define $O = (0 : 0 : 1)$ an inflection point on $E(\mathbb{K})$. We first map O to curve $E(\mathbb{K})_M$.

Let

$$\psi = (X : Y : Z) \longmapsto (U : V : W) = (U : \frac{af}{bg}U + W, V).$$

then with a little bit of help from mathematica, we have the following parameters:

$$\begin{aligned}
A &= a(a-b)f(af+bg),\\
B &= (a-b)bg(2af+bg)\,,\\
C &= b^3g^3\,,\\
D &= (a-b)b^2g^2.
\end{aligned}$$

Then, we obtain $E(\mathbb{K})_M = AU^3 + BU^2W + DUW^2 - CV^2W = 0$. One can note that E_M could be easily changed to the Weierstrass form. To return to Huffs elliptic curve from $E(\mathbb{K})_M$, one may apply the following map:

$$\psi^{-1} = (U : V : W) \longmapsto (X : Y : Z) = (X : Z : \frac{-af}{bg}X + Y).$$

It is noted that $(0 : 0 : 1)$ on E is mapped to $(0 : 1 : 0)$ on $E(\mathbb{K})_M$ through ψ.

To obtain the Weierstrass affine form, we let
$X = x$, $V = \frac{A}{C}y$ and $Z = \frac{C}{A}$ then we can simplify the equation

$$E(\mathbb{K})_M : y^2 = x^3 + \frac{BC}{A^2}x^2 + \frac{DC^2}{A^3}x.$$

After obtaining affine equation of E_M, we let $x = t + \frac{A}{BC}$ to get the following Weierstrass form equation,

$$E(\mathbb{K})_w : y^2 = t^3 + a_2t^2 + a_4t + a_6,$$

where

$$\begin{aligned} a_2 &= \frac{3A^3 + B^2C^2}{A^2BC}, \\ a_4 &= \frac{3A^5 + 2A^2B^2C^2 + B^2C^4D}{A^3B^2C^2}, \\ a_6 &= \frac{A^5 + A^2B^2C^2 + B^2C^4D}{A^2B^3C^3}. \end{aligned}$$

□

6 Computational cost analysis

Each coordinate systems cost is summarized in Table 1 for point addition and doubling point on standard coordinates for the elliptic curve (2.1).

Table 1: Computational cost comparison

Coordinates	Cost	
	Addition	Doubling
Projective	14m + 2s	13m + 5s
Jacobian	32m + 4s	29m + 5s
Lopez-Dahab	32m + 6s	26m + 5s
Embedding $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$	12m	6m + 4s

We note that the computational cost using the embedding $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$ is lowest than the projective, Jacobian, and Lopez Dahab coordinate systems. Thus, we recommend embedding $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$ system as the cost is lowest for point addition and doubling point on this curve.

To compare our results with other Huff's models, we have to take extra operations as a to be addition/subtraction of curve constants and d as multiplication by curve constants.

Table 2: Computational cost comparison of other forms of Huff's curve

Source and the curve equation	Addition	Doubling
Wu, Feng [33] plus assuming b=1, $X(aY^2 - Z^2) = Y(X^2 - Z^2)$	11m+d+14a	6m+5s+d+12a
Joye, Tibouchi, Vergnaud [22], $aX(Y^2 - Z^2) = bY(X^2 - Z^2)$	6m+5s+13a	11m+14a
Orhon and Hisil [29], $YT(Z^2 + 2X^2) = cXZ(T^2 + 2Y^2)$	10m+14a	8m+10a
Orhon and Hisil [29], $YT(Z^2 + X^2) = cXZ(T^2 + 2Y)$	10m+12a	8m+8a
This work using projective coordinate, $aX(Y + XY + fZ^2) = bY(X^2 + XY + gZ^2)$	14m+2s+2d+12a	13m+5s+2d+3a
This work by embedding $aXZ(Y^2 - cT^2) = bTY(X^2 - dZ^2)$ into $\mathbb{P}^1 \times \mathbb{P}^1$	12m+6a+4d	6m+4s+4a+4d

We note that the computational cost on the curves described in this paper is nearly optimal to other known Huff's model of elliptic curves [See in Table 2]. The results shown by Ciss and Sow on their curves [10] could be improved from $7m + 5s + 4a + 4d$ to $6m + 4s + 4a + 4d$ for the doubling point by embedding the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system.

7 Conclusion

In this paper, we have introduced a new form of elliptic curves in generalized Huff's model. We have presented formulae for point addition and doubling on affine, projective, Jacobian, Lopez-Dahab coordinates, and embedding of the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system. We have observed that the computational cost for point addition and doubling point on the new form of Huff's model of elliptic curves is lowest by embedding the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system than other mentioned coordinate systems. The results shown by Ciss and Sow on their curves have been improved from $7m + 5s + 4a + 4d$ to $6m + 4s + 4a + 4d$ for the doubling point by embedding the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system. The computational cost of the new form of Huff's curves is nearly optimal to other known Huff's models. We leave it as future work for a concrete computational cost comparison with other Huff's, Weierstrass, Montgomery, and Edwards curves. Furthermore, one can extend the study to supersingular elliptic curves and isogeny-based cryptography.

References

[1] C. Arene, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster computation of the tate pairing. *Journal of number theory*, 131(5):842–857, 2011.

[2] D. Bernstein, P. Birkner, T. Lange, and C. Peters. Ecm using edwards curves. *Mathematics of Computation*, 82(282):1139–1179, 2013.

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

[4] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted edwards curves. In *International Conference on Cryptology in Africa*, pages 389–405. Springer, 2008.

[5] D. J. Bernstein, T. Lange, and R. R. Farashahi. Binary edwards curves. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 244–265. Springer, 2008.

[6] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange. Twisted hessian curves. In *International Conference on Cryptology and Information Security in Latin America*, pages 269–294. Springer, 2015.

[7] O. Billet and M. Joye. The jacobi model of an elliptic curve and side-channel analysis. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 34–42, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg. ISBN 978-3-540-44828-0.

[8] J. Bos, C. Costello, P. Longa, and M. Naehrig. Specification of curve selection and supported curve parameters in msr ecclib. Technical report, Technical Report MSR-TR-2014-92, Microsoft Research, 2014.

[9] J. W. Bos, C. Costello, P. Longa, and M. Naehrig. Selecting elliptic curves for cryptography: An efficiency and security analysis. *Journal of Cryptographic Engineering*, 6(4): 259–286, 2016.

[10] A. A. Ciss and D. Sow. On a new generalization of huff curves. *IACR Cryptology ePrint Archive*, 2011:580, 2011.

[11] M Prem Laxman Das and Palash Sarkar. Pairing computation on twisted edwards form elliptic curves. In *International Conference on Pairing-Based Cryptography*, pages 192–210. Springer, 2008.

[12] J. Devigne and M. Joye. Binary huff curves. In *Cryptographers Track at the RSA Conference*, pages 340–355. Springer, 2011.

[13] H. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44(3):393–422, 2007.

[14] S. D. Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, 2012.

[15] P. Gallagher. Digital signature standard (dss). *Federal Information Processing Standards Publications, volume FIPS*, pages 186–3, 2013.

[16] H. Hasse. Zur theorie der abstrakten elliptischen funktionenkï¿œrper iii. die struktur des meromorphismenrings. die riemannsche vermutung. *Journal fï¿œr die reine und angewandte Mathematik*, 175:193–208, 1936. URL `http://eudml.org/doc/149968`.

[17] X. He, W. Yu, and K. Wang. Hashing into generalized huff curves. In *International Conference on Information Security and Cryptology*, pages 22–44. Springer, 2015.

[18] Gerald B Huff. Diophantine problems in geometry and elliptic ternary forms. *Duke Mathematical Journal*, 15(2):443–453, 1948.

[19] S. Ionica and A. Joux. Another approach to pairing computation in edwards coordinates. In *International Conference on Cryptology in India*, pages 400–413. Springer, 2008.

[20] Terence Jackson. Lectures on elliptic curves, london mathematical society student texts 24, by jws cassels. pp 137.£ 13-95 (paper)£ 27-95 (hard). 1991. isbn 0-521-42530-1,-41517-9.(cambridge university press). *The Mathematical Gazette*, 79(484):216–216, 1995.

[21] M. Joye and J. Quisquater. Hessian elliptic curves and side-channel attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 402–410. Springer, 2001.

[22] M. Joye, M. Tibouchi, and D. Vergnaud. Huff's model for elliptic curves. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory*, pages 234–250, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. ISBN 978-3-642-14518-6.

[23] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[24] N. Koblitz and A. J. Menezes. A survey of public-key cryptosystems. *SIAM review*, 46(4): 599–634, 2004.

[25] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231. Springer, 1978.

[26] V. S. Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

[27] Peter L Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.

[28] Trygve Nagell. Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Mathematica*, 52(1):93–126, Dec 1929. ISSN 1871-2509. doi: 10.1007/BF02592681. URL `https://doi.org/10.1007/BF02592681`.

[29] Neriman Gamze Orhon and Huseyin Hisil. Speeding up huff form of elliptic curves. *Designs, Codes and Cryptography*, 86(12):2807–2823, 2018.

[30] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[31] Mehdi Tibouchi. A nagell algorithm in any characteristic. In *Cryptography and Security: From Theory to Applications*, pages 474–479. Springer, 2012.

[32] A. Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141 (3):443–551, 1995.

[33] H. Wu and R. Feng. Elliptic curves in huff's model. *Wuhan University Journal of Natural Sciences*, 17(6):473–480, Dec 2012. ISSN 1993-4998. doi: 10.1007/s11859-012-0873-9. URL `https://doi.org/10.1007/s11859-012-0873-9`.