Elliptic Curves in Generalized Huff's Model

NutMiC 2019

Ronal Pranil Chand * Maheswara Rao Valluri *

June 24, 2019

* School of Mathematical & Computing Sciences, Fiji National University (FNU), Fiji.

Objective

- To propose a new curve which is a generalization of Huff's model of elliptic curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$.
- To show that the curve $E(\mathbb{K})$ is a group under addition ($\oplus$).
- To provide formulae for point addition and doubling point in affine and projective coordinate systems.
- Compute computational cost of point addition and doubling points in affine, projective, Jacobian and Lopez-Dahab coordinates.
- Compare the computional cost of projective, Jacobian and Lopez-Dahab coordinates.

Background

- 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 $\mathbb{K}$.
- Elliptic curves are studied in various areas such as Algebra, Algebraic Geometry and Number Theory.
- Elliptic curves for its usefulness are widely used in the construction of cryptosystem.
- In 1948 Huff Gerald introduced the elliptic curve of the form

$$ax(y^2-1)=by(x^2-1), \text{where } a^2-b^2\neq 0.$$

.

Families of Huff's Elliptic Curves

- The curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Huff.1948 are of the form of:

$$ax(y^2 - 1) = by(x^2 - 1), \text{where } a^2 - b^2 \neq 0.$$

- The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Joye et al.2010 are of the form of:

$$ax(y^2 - d) = by(x^2 - d), \text{where } abd(a^2 - b^2) \neq 0.$$

- The generalized Huff's curves over a field $\mathbb{K}$. char($\mathbb{K}$) $\neq 2$ by Wu and Feng.2010 are of the form of:

$$x(ay^2 - 1) = y(bx^2 - 1), \text{where } ab(a - b) \neq 0.$$

...continued

- The binary Huff curves over a field $\mathbb{K}$, char($\mathbb{K}$) $= 2$ by Joye et al.2010 are of the form of:

$$ax(y^2 + y + 1) = by(x^2 + x + 1), \text{where } ab(a - b) \neq 0.$$

- The generalized binary Huff curves over a field $\mathbb{K}$, char($\mathbb{K}$) $= 2$ by Joye et al.2010 are of the form of:

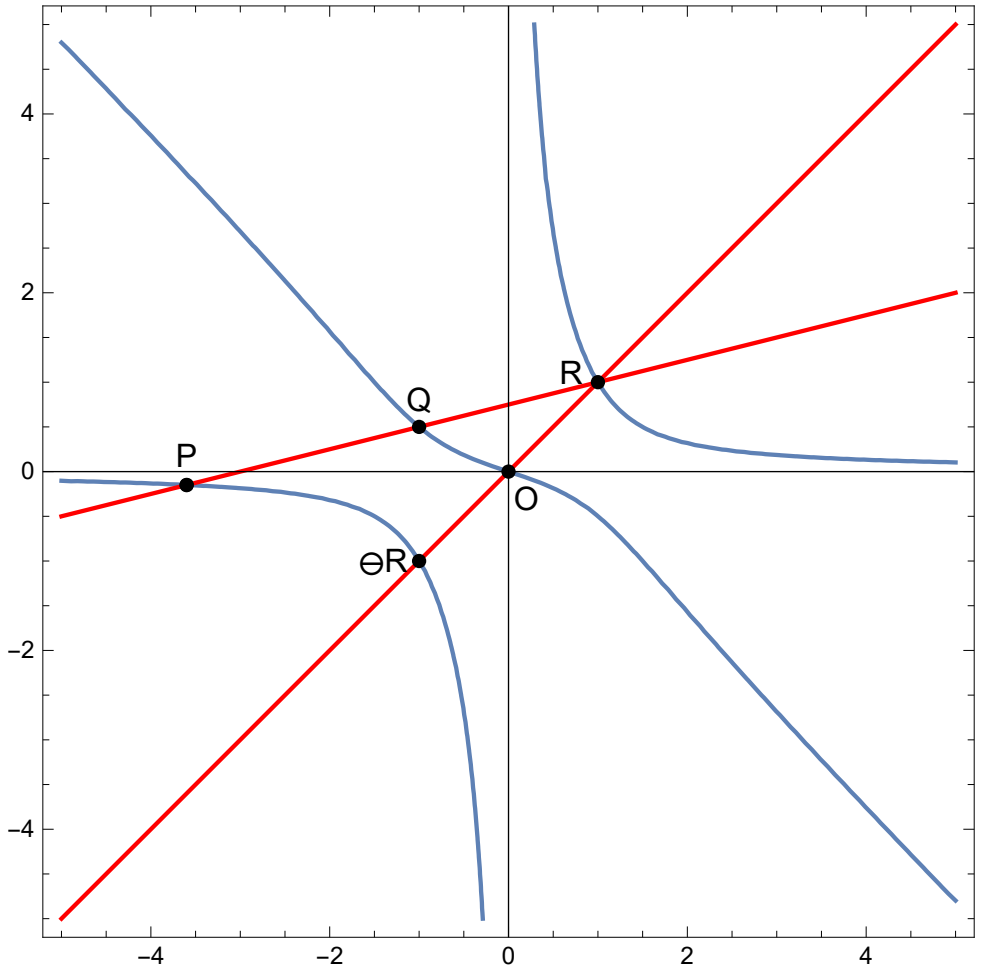
$$ax(y^2 + fy + 1) = by(x^2 + fx + 1), \text{where } abf(a - b) \neq 0.$$

- The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Ciss and Sow.2011 are of the form of:

$$ax(y^2 - c) = by(x^2 - d), \text{where } abcd(a^2c - b^2d) \neq 0.$$

Generalized Huff's Model

- The new generalized curves 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 $abfg(a - b) \neq 0$.



- The secant line $y = \lambda x + \beta$ joining P and Q have the slope defined as $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.
- The coordinates of R simplifies to

$$x_3 = -\frac{(x_1 - x_2)\left(y_1\left(x_1 + y_1\right) - y_2\left(x_2 + y_2\right)\right)}{(y_1 - y_2)\left(x_1 - x_2 + y_1 - y_2\right)}$$

and

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

- Point $R = (x_3, y_3)$ is computed by the above formulae only if $x_1 \neq x_2$, $y_1 \neq y_2$ and $x_1 - x_2 + y_1 - y_2 \neq 0$.

For the points $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, y_3)$ on $E(\mathbb{K})$.

- Addition of any two points gives the inverse of the third point such that $P \oplus Q = \ominus R$ and $Q \oplus R = \ominus P$.
- Associative property:For $P \oplus (Q \oplus R) = P \ominus P$

$$\begin{aligned} x_A &= -\frac{(x_1 - -x_1)\left(y_1\left(x_1 + y_1\right) - -y_1\left(-x_1 - y_1\right)\right)}{(y_1 - -y_1)\left(x_1 - -x_1 + y_1 - -y_1\right)} \\ &= -\frac{(2x_1)\left(x_1y_1 + y_1^2 + -x_1y_1 - y_1^2\right)}{(2y_1)\left(2x_1 + 2y_1\right)} \\ &= 0. \end{aligned}$$

$$\begin{aligned} y_A &= -\frac{(y_1 - -y_1)\left(x_1^2 + x_1y_1 - -x_1\left(-x_1 - y_1\right)\right)}{(x_1 - -x_1)\left(x_1 - -x_1 + y_1 - -y_1\right)} \\ &= -\frac{(2y_1)\left(x_1^2 + x_1y_1 - x_1^2 - x_1y_1\right)}{(2x_1)\left(2x_1 + 2y_1\right)} \\ &= 0. \end{aligned}$$

and for $(P \oplus Q) \oplus R) = \ominus R \oplus R$.

$$\begin{aligned} x_A &= -\frac{(x_3 - -x_3)\,(y_3\,(x_3 + y_3) - -y_3\,(-x_3 - y_3))}{(y_3 - -y_3)\,(x_3 - -x_3 + y_3 - -y_3)} \\ &= -\frac{(2x_3)\left(x_3y_3 + y_3^2 + -x_3y_3 - y_3^2\right)}{(2y_3)\,(2x_3 + 2y_3)} \\ &= 0. \end{aligned}$$

$$\begin{aligned} y_A &= -\frac{(y_3 - -y_3)\left(x_3^2 + x_3y_3 - -x_3\,(-x_3 - y_3)\right)}{(x_3 - -x_3)\,(x_3 - -x_3 + y_3 - -y_3)} \\ &= -\frac{(2y_3)\left(x_3^2 + x_3y_3 - x_3^2 - x_3y_3\right)}{(2x_3)\,(2x_3 + 2y_3)} \\ &= 0. \end{aligned}$$

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

- $P \oplus O$ could be obtained by point addition formulae as follows:

$$\begin{aligned} x_3 &= -\frac{(x_1-0)\,(y_1\,(x_1+y_1)-0\,(0+0))}{(y_1-0)\,(x_1-0+y_1-0)}. \\ &= -\frac{x_1y_1\,(x_1+y_1)}{y_1\,(x_1+y_1)} \\ &= -x. \end{aligned}$$

and

$$\begin{aligned} y_3 &= -\frac{(y_1-0)\left(x_1^2+x_1y_1-0\,(0+0)\right)}{(x_1-0)\,(x_1-0+y_1-0)}. \\ &= -\frac{y_1\left(x_1^2+x_1y_1\right)}{(x_1)\,(x_1+y_1)} \\ &= -y. \end{aligned}$$

Thus $P \oplus O = -(-x_1, -y_1) = P$. Thus $E(\mathbb{K})$ is group.

Doubling Point $(2P)$

For

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

and

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

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

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

Projective formulae

- There are three points at infinity, namely $(1,0,0)$, $(0,1,0)$ and $(a,b,0)$ on $E(\mathbb{K})$
- The sum of any two points at infinity equals to the third point.
- The projective form of the curve equation is $E(\mathbb{K}) : aX\left(Y^2+XY+fZ^2\right) = bY\left(X^2+XY+gZ^2\right).$
- To get coordinates for point addition and doubling point we let $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ and $Z = 1$
- Point addition for projective form is as

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

- For doubling point

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

continue...

- To get the Jacobian coordinates for addition and doubling point we replace $x = \frac{X}{Z^2}$, $y = \frac{Y}{Z^3}$ and $Z = 1$.
- To get the Lopez-Dahab coordinates for addition and doubling point we replace $x = \frac{X}{Z}$, $y = \frac{Y}{Z^2}$ and $Z = 1$.
- Table 1 shows the total computational cost of each mentioned coordinate system,

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

.

Conclusion

- Generalized Huff's elliptic curves satisfy group properties.
- Additional and doubling point of projective, Jacobian and Lopez-Dahab coordinates were computed.
- Projective coordinates have lower commotional costs than other mentioned coordinates.
- It remains to conduct a comparative study for the point addition and doubling point to mentioned curves.

THANK YOU