Alexander Rostovtsev
St. Petersburg State Polytechnic University
rostovtsev@ssl.stu.neva.ru

Linear equivalence between elliptic curves in Weierstrass and Hesse form

Abstract

Elliptic curves in Hesse form admit more suitable arithmetic than ones in Weierstrass form. But elliptic curve cryptosystems usually use Weierstrass form. It is known that both those forms are birationally equivalent. Birational equivalence is relatively hard to compute. We prove that elliptic curves in Hesse form and in Weierstrass form are linearly equivalent over initial field or its small extension and this equivalence is easy to compute. If cardinality of finite field $q \equiv 2 \pmod 3$ and Frobenius trace $T \equiv 0 \pmod 3$, then equivalence is defined over initial finite field. This linear equivalence allows multiplying of an elliptic curve point in Weierstrass form by passing to Hessian curve, computing product point for this curve and passing back. This speeds up the rate of point multiplication about 1,37 times.

1. Introduction

Let $\mathbb{F}_q$ is field of $q = p^n$ elements for prime p and $\overline{\mathbb{F}_q}$ is its algebraic closure. Projective plane is set of points given by triples $(X, Y, Z)\backslash(0, 0, 0)$ with equivalence $(X, Y, Z) = (uX, uY, uZ)$ for any $u \in \overline{\mathbb{F}_q^*}$. Points with $Z = 0$ are points of infinity.

Projective algebraic curve is subset of projective plain where polynomial $f(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ takes zero. Affine algebraic curve is subset of projective curve with $Z \neq 0$. If $\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = L \begin{pmatrix} U \\ V \\ W \end{pmatrix}$, where L is invertible matrix, and $f(X, Y, Z) = g(U, V, W)$, then curves given by polynomial f, g are linearly equivalent and $\deg(f) = \deg(g)$.

If between two polynomials f, g there exist rational maps φ, ψ so that $f = \varphi(g)$, $g = \psi(f)$, and $\varphi\psi$ and $\psi\varphi$ are identity maps (if they are defined) on corresponding curves, then curves given by polynomial f, g are birationally equivalent. Birational equivalence can be partially determined and it can change degree of polynomial. If such maps φ, ψ between affine curves are polynomial, curves are isomorphic. Linear equivalence that maps points of infinity to points of infinity defines isomorphism of algebraic curves.

Elliptic curve is smooth projective cubic curve. Elliptic curves over finite fields are widely used in public key cryptography. Such curves can be given by different polynomials. The most common one is polynomial in Weierstrass form

$$E_W(\mathbb{F}_q)\colon Y^2Z - X^3 - AXZ^2 - BZ^3 \tag{1}$$

if $p \geq 5$. This curve has the flex at infinity $P_\infty = (0, 1, 0)$. Elliptic curve in Hesse form is given by polynomial

$$E_H(\mathbb{F}_q)\colon U^3 + V^3 + W^3 - 3mUVW \tag{2}$$

where $p \neq 3$ and $m^3 \neq 1$. This curve has three flexes at infinity $P_\infty = (1, -1, 0)$, $(1, -\rho, 0)$ and $(1, -\rho^2, 0)$, $\rho = \dfrac{-1+\sqrt{-3}}{2}$ (if -3 is a square), or only one flex P_∞ (if -3 is not a square).

Elliptic curve up to isomorphism (over $\mathbb{F}_q$ or its finite extension) is defined by its j-invariant, $j = \dfrac{2^8 3^3 A^3}{4A^3 + 27B^2}$ for curve (1) and $j = \left(\dfrac{3m(8+m^3)}{-1+m^3} \right)^3$ for curve (2).

Points of elliptic curves form Abelian group with addition low

$$(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3).$$

For curve (1) opposite to (X, Y, Z) is $(X, -Y, Z)$, zero element is P_∞ and sum of two points is given by polynomials of degree 6

$$X_3 \equiv 2Y_1Z_1((3X_1^2 + AZ_1^2)^2 - 8X_1Y_1^2Z_1),$$
$$Y_3 \equiv 4Y_1^2Z_1(3X_1(3X_1^2 + AZ_1^2) - 2Y_1^2Z_1) - (3X_1^2 + AZ_1^2)^3,$$
$$Z_3 \equiv 8Y_1^3Z_1^3$$

if $(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$ and by polynomials of degree 8

$$X_3 \equiv (X_2Z_1 - X_1Z_2)(Z_1Z_2(Y_2Z_1 - Y_1Z_2)^2 - (X_2Z_1 + X_1Z_2)(X_2Z_1 - X_1Z_2)^2),$$
$$Y_3 \equiv (X_2Z_1 - X_1Z_2)^2(Y_2Z_1(X_2Z_1 + 2X_1Z_2) - Y_1Z_2(X_1Z_2 + 2X_2Z_1)) - Z_1Z_2(Y_2Z_1 - Y_1Z_2)^3,$$
$$Z_3 \equiv Z_1Z_2\,(X_2Z_1 - X_1Z_2)^3$$

if $(X_1, Y_1, Z_1) \neq (X_2, Y_2, Z_2)$.

The most hard operation during elliptic curve point doubling or point addition is field multiplication and squaring, because its complexity is $O(\log q)^2$, but complexity of addition and subtraction is $O(\log q)$. So we can estimate the complexity of elliptic curve arithmetic as number of field multiplications.

Point doubling takes 13 field multiplications (12 for $A = \pm 1$). If one point is fixed with $Z = 1$, point addition takes 12 field multiplications.

For curve (2) opposite to (U, V, W) is (V, U, W), zero element is P_∞. Sum of points is given by polynomials of degree 4

$$U_3 = V_1(W_1^3 - U_1^3),$$

$$V_3 = U_1(V_1^3 - W_1^3),$$
$$W_3 = W_1(U_1^3 - V_1^3)$$

if $(U_1, V_1, W_1) = (U_2, V_2, W_2)$ and

$$U_3 = U_1W_1V_2^2 - U_2W_2V_1^2,$$
$$V_3 = V_1W_1U_2^2 - V_2W_2U_1^2,$$
$$W_3 = U_1V_1W_2^2 - U_2V_2W_1^2$$

if $(U_1, V_1, W_1) \neq (U_2, V_2, W_2)$. Point doubling takes 9 field multiplications. If one of two summand points is fixed and has $W = 1$, point addition takes 10 field multiplications.

In spite of some improvements curve in Hesse form admits more fast arithmetic then ones in Weierstrass form [3]. Elliptic curve digital signature algorithm [2] use elliptic curves in Weierstrass form (1).

M. Ciet, G. Piret and J.-J. Quisquater in [1], M. Joyee and J.-J. Quisquater in [4] show that there exists birational isomorphism between Weierstrass and Hesse form. This map is not common for computing. The aim of this paper is to show that there exists common linear equivalence between elliptic curves (1) and (2) and this equivalence is defined over initial field or over its finite extension, and to recognize whether the equivalence exists over initial finite field. This equivalence can speed-up arithmetic of elliptic curve in Weierstrass form. Besides of that it gives simple formulas for complex multiplication on elliptic curve in Hesse form.

In section 2 the existence of linear equivalence is proved, in section 3 we consider when this equivalence is defined over initial field, in section 4 we consider application of the equivalence theorem.

2. Elliptic curve linear equivalence

Theorem 1. Let field characteristic differs from 2, 3. Elliptic curves $E(\mathbb{F}_q)$ for given polynomials (1) and (2) are linearly equivalent over $\overline{\mathbb{F}_q}$. Linear map from (2) to (1) exists over $\mathbb{F}_q$. Linear map from (1) to (2) exists over $\mathbb{F}_q$ or over its extension of degree 2, 3, 4 or 6.

Proof. Linear map from (2) to (1) is $L = \begin{pmatrix} m & 1 & \frac{4-m^3}{3} \\ m & -1 & \frac{4-m^3}{3} \\ -2 & 0 & -2m^2 \end{pmatrix}$. Matrix determinant is $\frac{16(-1+m^3)}{3}$. It is invertible if $p \neq 2, 3$ and is defined over initial

field. Inverse linear map from (1) to (2) is $M = \begin{pmatrix} m^2 & m^2 & \frac{4-m^3}{3} \\ \frac{-4+4m^3}{3} & \frac{4-4m^3}{3} & 0 \\ -1 & -1 & -m \end{pmatrix}$ (for simplicity M is product of L^{-1} and scalar matrix).

Invariant j is a cube in initial field [5]. Let $j = \gamma_2^3$. Equation $\gamma_2 = \frac{3m(8+m^3)}{-1+m^3}$ can have 0, 1, 2 or 4 roots in $\mathbb{F}_q$. Its splitting field k has degree over $\mathbb{F}_q$ 4, 3, 2 or 1 correspondingly. Equation $j = \left(\frac{3m(8+m^3)}{-1+m^3} \right)^3$ is equivalent to equation

$$(\gamma_2(-1 + m^3))^3 = (3m(8 + m^3))^3. \quad (3)$$

Its roots are in k or in quadratic extension of k if $\sqrt{-3} \notin k$. Notice that if degree of k over $\mathbb{F}_q$ is even, then $\sqrt{-3} \in k$. So splitting field of equation (3) has degree over $\mathbb{F}_q$ 1, 2, 3, 4 or 6.

The image of Hesse curve is

$$Y^2Z - X^3 + \frac{m(8+m^3)XZ^2}{3} - \frac{2(-8-20m^3+m^6)Z^3}{27}. \quad (4)$$

Linear equivalence does not change invariant j. **n**

Theorem 2. Let $E_2 = \varphi(E_1)$ is invertible linear map of elliptic curves and ψ: $E_1 \to E_1$ is invertible map given by homogenous polynomials of degree d. Then linear equivalence defines invertible map $\varphi\psi\varphi^{-1}$ of curve E_2 given by homogenous polynomials of degree d.

Proof. Map $\varphi\psi\varphi^{-1}$ acts on E_2 and it is invertible as product of invertible maps. Since φ is linear map, map $\varphi\psi\varphi^{-1}$ is given by polynomials of degree $\le d$. Assumption that degree is less then d leads to contradiction, because corresponding map $\psi = \varphi^{-1}(\varphi\psi\varphi^{-1})\varphi$ on E_1 will be given by polynomials of degree less then d. **n**

Corollary 3. If group order is odd integer, then there exist homogenous polynomials of degree 4 that give point doubling and point addition on elliptic curve in Weierstrass form.

Proof. If group order is odd, then point doubling is invertible map. Elliptic curve doubling and addition in Hesse form is defined by polynomials of degree 4. Apply theorems 1 and 2. **n**

3. Linear equivalence over initial field

Consider whether linear map $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ is defined over $\mathbb{F}_q$. Existence of the linear map is equivalent to existence of Hessian elliptic curve with the same number of points and the same j-invariant as elliptic curve in Weierstrass form.

Let $q \equiv 2 \pmod 3$, then each element of $\mathbb{F}_q$ is a cube, so map $\gamma_2 \to \gamma_2^3 = j$ is bijection. If m runs through $\mathbb{F}_q$, number of impossible j for Hessian curve equals to number of impossible γ_2. Equation

$$\gamma_2(-1 + m^3) = 3m(8 + m^3) \tag{5}$$

has 4 solutions over $\overline{\mathbb{F}_q}$:

$$\frac{1}{12}\left(\gamma_2 \pm \sqrt{(6+\gamma_2)^2+108} \pm \sqrt{2(12-\gamma_2)\left(-6-\gamma_2 \pm \sqrt{(6+\gamma_2)^2+108}\right)} \right),$$

where signs of $\sqrt{(6+\gamma_2)^2+108}$ change simultaneously in both positions.

Equation (5) is linearly equivalent to biquadratic equation $x^4 + 2ax^2 + b = 0$ if

$$a = \frac{6\gamma_2 + \alpha - 12\sqrt{\alpha} - \gamma_2\sqrt{\alpha}}{18},\ b = \frac{-\gamma_2^2 - 6\sqrt{\alpha} + \gamma_2\sqrt{\alpha}}{36},\ \alpha = (6 + \gamma_2)^2 + 108.$$

Its solutions are $\pm\sqrt{-a \pm \sqrt{a^2 - b}}$. Hence $\alpha = (6 + \gamma_2)^2 + 108$ is a square in $\mathbb{F}_q$.

Equation (5) has solution is in $\mathbb{F}_q$ if terms $\sqrt{(6+\gamma_2)^2+108}$ and $\sqrt{2(12-\gamma_2)\left(-6-\gamma_2 \pm \sqrt{(6+\gamma_2)^2+108}\right)}$ both are in $\mathbb{F}_q$. In this case there are two solutions. Linear equivalence between equation (5) and the biquadratic equation means that if one term is in $\mathbb{F}_q$, then other term is in $\mathbb{F}_q$ too. Its probability is ≈ 0.5. Required elliptic curve exists if $(6 + \gamma_2)^2 + 108$ is a square. The two roots correspond to twisted elliptic curves which have the same j but opposite traces of Frobenius endomorphism.

Theorem 4. If $q \equiv 2 \pmod 3$, then Hessian elliptic curve has trace of Frobenius endomorphism $T \equiv 0 \pmod 3$.

Proof. Hessian elliptic curve over arbitrary field has affine flex $(0, -1, 1)$ of order 3. Hence its number of points over finite field $N \equiv 0 \pmod 3$. Trace of Frobenius endomorphism is defined as $T = q + 1 - N$. Substituting $q \equiv 2 \pmod 2$, gives $T \equiv 0 \pmod 3$. **n**

Linear map $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ is defined over $\mathbb{F}_q$ if equalities obtained in theorem 1 hold simultaneously

$$A = -\frac{m(8+m^3)}{3},\ B = \frac{2(-8-20m^3+m^6)}{27}.$$

With probability near to 1 there is no such m. But parameter m can de found using usual Weierstrassian elliptic curve isomorphism $(X, Y, Z, A, B) \to (u^2X, u^3Y, Z, u^4A, u^6B)$ for arbitrary $u \neq 0$. Then equations are transformed:

$$u^4 A = -\frac{m(8+m^3)}{3}, \quad u^6 B = \frac{2(-8-20m^3+m^6)}{27}. \tag{6}$$

If $q \equiv 5 \pmod 6$ and Weierstrassian elliptic curve $E_W(\mathbb{F}_q)$ has $T \equiv 0 \pmod 3$, then there exists linearly equivalent Hessian elliptic curve $E_H(\mathbb{F}_q)$. Equations (6) have solutions $(m, \pm u)$ in $\mathbb{F}_q$ if and only if equation (5) has solution in $\mathbb{F}_q$. It was shown above that $(6 + \gamma_2)^2 + 108$ is a square in $\mathbb{F}_q$ and equation (5) has required solution. Hence equations (6) have solution in $\mathbb{F}_q$ too. Linear equivalence between elliptic curves in Weierstrass and Hesse form is defined over $\mathbb{F}_q$ and is given by equations

$$\begin{aligned} U &= u^2 mX + u^3 Y + \frac{4-m^3}{3} Z, \\ V &= u^2 mX - u^3 Y + \frac{4-m^3}{3} Z, \\ W &= -2u^2 X - 2m^2 Z, \end{aligned} \tag{7}$$

$$\begin{aligned} X &= u^{-2}\left(m^2(U+V) + \frac{4-m^3}{3} W\right), \\ Y &= u^{-3}\frac{4-m^3}{3}(-U+V), \\ Z &= -U-V-mW. \end{aligned} \tag{8}$$

If $q \equiv 1 \pmod 3$, then cubing is not a bijection. There exists $\rho = \frac{-1+\sqrt{-3}}{2} \in \mathbb{F}_q$, and Hessian elliptic curve has 9 points of order 3. Group of points of order 3 is direct sum of two cyclic groups of order 3. Hence number of points satisfies congruence $N \equiv 0 \pmod 9$. Linear map $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ may be determined over extension of initial field. Notice that Hessian elliptic curve $E_H(\mathbb{F}_q)$ can correspond only to one of two twisted Weierstrassian elliptic curves. So case $q \equiv 1 \pmod 3$ has less practical interest than case $q \equiv 2 \pmod 3$.

4. Applications of linear equivalence

Given linear equivalence can be used both directly (transformation Weierstrass curve to Hesse curve, multiplication point by a number and back transformation) and for determining complex multiplication formulas, which allow speeding-up computations. Consider some examples.

1. Hessian elliptic curve has $j = 0$ and is isomorphic to curve $Y^2Z - X^3 - BZ^3$ if $m = 0, -2$. Last curve has complex multiplication by $\frac{1+\sqrt{-3}}{2}$:

$$\left(\frac{1+\sqrt{-3}}{2}\right)(X,Y,Z) = (\rho X, -Y, Z),\ \rho = \frac{-1+\sqrt{-3}}{2}.$$

If $m = 0$ linear map and its inverse are given by matrices

$$\begin{pmatrix} 0 & 1 & 4/3 \\ 0 & -1 & 4/3 \\ -2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 4 \\ -4 & 4 & 0 \\ -3 & -3 & 0 \end{pmatrix}.$$

Isomorphic image of Hesse curve has coefficient $B = -16/27$. Corresponding complex multiplication of Hesse curve is linear map

$$\frac{1+\sqrt{-3}}{2}(X,Y,Z) = (Y, X, \rho Z).$$

2. Hessian elliptic curve has $j = 1728$ and is isomorphic to curve $Y^2Z - X^3 - AXZ^2$ if $m = 1+\sqrt{3}$. Last curve has possesses complex multiplication by $\sqrt{-1}$: $\sqrt{-1}(X,Y,Z) = (-X, \sqrt{-1}Y, Z)$. Isomorphic image of Hesse curve has coefficient $A = -4(3+2\sqrt{3})$. Corresponding complex multiplication of Hesse curve is linear map

$$\sqrt{-1}(X,Y,Z) = (\rho X + \rho^2 Y + Z, \rho^2 X + \rho Y + Z, X + Y + Z).$$

3. Hessian elliptic curve has $j = 8000$ and is isomorphic to curve $Y^2Z - (X^3 - 4tX^2Z + 2t^2XZ^2)$ if $m = \frac{-2-\sqrt{-2}}{3}$. Last curve has complex multiplication defined by isogeny of degree 2:

$$\sqrt{-2}(X,Y,Z) = \left(-Y^2Z, \frac{Y(X^2 - 2t^2Z^2)}{\sqrt{-2}}, 2X^2Z\right).$$

Point (0, 0) has order 2 and is in the isogeny kernel. This curve can be transformed to (1) by substitution $X \leftarrow X + \frac{4t}{3}Z$, then polynomial (1) has coefficients $A = -\frac{10}{3}t^2$, $B = -\frac{56}{27}t^3$. Required m is obtained if $t = \frac{-2+5\sqrt{-2}}{9}$. Corresponding complex multiplication on Hesse curve is defined by homogenous cubic polynomials.

4. Multiplication of a point of Weierstrassian elliptic curve by a number.

In cryptographic applications group order is large prime. According to corollary 3, point doubling and point addition on Weierstrass elliptic curve can be defined by homogenous polynomials of degree 4 instead of well-known polynomials of degree 6, 8. It is sufficient to transform Weierstrass curve to Hesse form, do point doublings/additions and make inverse transformation.

Computing linear equivalence and its inverse takes 9 field multiplications. Linear map $E_W(\mathbb{F}_q) \to E_H(\mathbb{F}_q)$ according to (7) takes 5 field multiplications: u^2mX, $-2u^2X$, u^3Y, $\frac{4-m^3}{3}Z$, $-2m^2Z$. Inverse linear map $E_H(\mathbb{F}_q) \to E_W(\mathbb{F}_q)$ according to (8) takes 4 field multiplications: $u^{-2}m^2(U+V)$, $\frac{4-m^3}{3u^2}W$, $\frac{4-4m^3}{3u^3}(-U+V)$, mZ. If group order size n = 160 bits, complexity of linear maps computation is negligible comparatively to complexity of point multiplication. The signed binary window method takes at average $n - 1$ point doublings and $(n - 1)/3$ point additions, so it takes $159 \cdot 13 + 53 \cdot 12 = 2703$ field multiplications. Proposed method takes $9+159 \cdot 9 + 53 \cdot 10 = 1970$ field multiplications and the rate of Weierstrassian elliptic curve point multiplication increases about 1.37 times.

According to ECDSA signature generation takes point multiplication, and x-coordinate of this point is a part of signature. Since $x = XZ^{-1}$, one can compute only two coordinates X and Z of a point of Weierstrassian curve in (8) instead of three coordinates.

References

1. M. Ciet, G. Piret and J.-J Quisquater, *Several optimizations for elliptic curve implementation on smart card* // Universite Catholique de Louvain, Technical report CG-2001/1, Available at: http://www.dice.ucl.ac.be/crypto/
2. FIPS 186-2, *Digital signature standard* (*DSS*), National Institute of Standards and Technology, USA, 2000.
3. H. Hisil, K. Wong, G. Carter, E. Dawson, *Faster group operations on elliptic curves* // International Association for Cryptologic Research, Cryptology ePrint Archive // http://eprint.iacr.org/2007/441.
4. M. Joye and J.-J Quisquater, *Hessian elliptic curves and side channel attacks* // Proceedings of CGES 2001, LNCS, v. 2162, Springer-Verlag, 2001, pp. 402-410.
5. J. Silverman, *Advances topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, New York, 1994.