The geometry of efficient arithmetic on elliptic curves

David Kohel
Institut de Mathématiques de Luminy

Geocrypt 2013 (Tahiti)
7 October 2013

Elliptic curve models

An *elliptic curve* E is a projective nonsingular genus one curve with a fixed base point O. In order to consider the arithmetic, namely addition and scalar multiplication defined in terms of polynomial maps, we need to fix the additional structure of a projective embedding $\iota : E \longrightarrow \mathbb{P}^r$, which we call a *projective model*.

We suppose that the model is given by a complete linear system. Letting $\{X_0, \ldots, X_r\}$ be the coordinate functions on $\mathbb{P}^r$, we obtain a ring surjection:

$$\iota^* : k[\mathbb{P}^r] = k[X_0, \ldots, X_r] \longrightarrow k[E] = \frac{k[X_0, \ldots, X_r]}{I_E}.$$

We seek to analyze the role of the projective model in the efficient arithmetic of the curve.

The embedding class

The property that ι is given by a complete linear system lets us reduce to questions of sections of invertible sheaves. Specifically, let $\mathscr{L} = \iota^* \mathcal{O}_{\mathbb{P}^r}(1)$ the the sheaf giving the embedding, generated by coordinate functions $\{X_0, \ldots, X_r\}$. More generally, the global sections $\Gamma(E, \mathscr{L}^n)$ is the finite dimensional k-vector space spanned by monomials of degree n modulo I_E, and hence

$$k[E] = \bigoplus_{n=0}^{\infty} \Gamma(E, \mathscr{L}^n) \subset k(E)[X_0].$$

The *embedding class* of ι is characterized by its degree $d = r + 1$ and a point T in $E(k)$ such that for any hyperplane H,

$$E \cap H = \{P_0, \ldots, P_r\} \subset E(\bar{k}),$$

such that $P_0 + \cdots P_r = T$.

Riemann–Roch spaces

Let D be the divisor on E cut out by $X_0 = 0$, then we can identify $\Gamma(E, \mathscr{L}^n)$ with the Riemann–Roch space associated to nD:

$$L(nD) = \{f \in k(E)^* \mid \operatorname{div}(f) \geq -nD\} \cup \{0\},$$

more precisely, $\Gamma(E, \mathscr{L}^n) = L(nD)X_0^n \subset k(E)X_0^n$.

While the dimension of $L(nD)$ is nd, the dimension of the space of all monomials of degree n is:

$$\dim_k \left(\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n))\right) = \binom{n+r}{r} = \binom{n+d-1}{d-1}.$$

The discrepancy is accounted for by relations of a given degree in I_E. Specifically each polynomial in the quotient $\Gamma(E, \mathscr{L}^n) \subset k[E]$ represents a coset of polynomials of dimension

$$\binom{n+r}{r} - nd.$$

From the following table of dimensions:

	$d=3:$		$d=4:$		$d=5:$		$d=6:$	
n	$\binom{n+r}{r}$	nd	$\binom{n+r}{r}$	nd	$\binom{n+r}{r}$	nd	$\binom{n+r}{r}$	nd
1	3	3	4	4	5	5	6	6
2	6	6	10	8	15	10	21	12
3	10	9	15	12	35	15	56	18

we see the well-known result that a degree-3 curve in $\mathbb{P}^2$ is generated by a cubic relation, and a degree-4 curve in $\mathbb{P}^3$ is the intersection of two quadrics. Similarly, a quintic model in $\mathbb{P}^4$ and a sextic model in $\mathbb{P}^5$ are generated by a space of quadrics of dimensions 5 and 9, respectively.

When considering polynomial maps between curves, this space of relations is a source of flexibility for evaluating a representative polynomial f in its class.

Addition law relations

A similar analysis applies to the set of *addition laws* from $E \times E$ to E. The set polynomials of bidegree (m, n) on $E \times E$ are well-defined modulo relations of bidegree (m, n).

As the kernel of the surjective homomorphism

$$\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) \otimes_k \Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n)) \longrightarrow \Gamma(E, \mathscr{L}^m) \otimes_k \Gamma(E, \mathscr{L}^n)),$$

its dimension is

$$\binom{m+r}{r}\binom{n+r}{r} - mnd^2.$$

In particular, this space of relations will be of interest in the case in the case of minimal bigdegree $(m, n) = (2, 2)$ for addition laws, where it becomes:

$$\binom{d+1}{2}^2 - 4d^2 = \frac{d^2(d-3)(d+5)}{4}.$$

Linear classification of models

Hereafter we consider only projective models. A linear change of variables gives a model with equivalent arithmetic, up to multiplication by constants, thus it is natural to consider *linear isomorphisms* between models of elliptic curves.

Definition

Suppose that $E \subset \mathbb{P}^r$ is an elliptic curve model given by a complete linear system. Then any hyperplane H meets E in $r+1$ points $\{P_0, \ldots, P_r\}$, counting multiplicities. The point $T = P_0 + \cdots P_r$ is an invariant of the model called the *embedding class*.

Next we recall a result regarding the classification of elliptic curves models up to projective linear equivalence, in terms of its degree and embedding class.

Linear classification of models

Theorem

Let E_1 and E_2 be two models in $\mathbb{P}^r$, of degree $d = r + 1$, for an elliptic curve E, given by complete linear systems. There exists a linear transformation of $\mathbb{P}^r$ inducing an isomorphism of E_1 to E_2 if and only if E_1 and E_2 have the same embedding class.

Remark. The theorem is false if the isomorphism in the category of elliptic curves is weakened to an isomorphism of curves.

Corollary

Two projective models for an elliptic curve, given by complete linear systems of the same degree, have equivalent arithmetic up to multiplication by scalars if they have the same embedding divisor class.

Linear action of $[-1]$

A natural condition is to assume that $[-1]$ is also linear on E in its embedding, for which we recall the notion of a symmetric model.

Definition

An elliptic curve model $\iota : E \to \mathbb{P}^r$ given by a complete linear system is *symmetric* if and only if any of the following is true:

1. $[-1]$ is given by a projective linear transformation,
2. $[-1]^*\mathscr{L} \cong \mathscr{L}$ where $\mathscr{L} = \iota^*\mathcal{O}_{\mathbb{P}^r}(1)$,
3. $T \in E[2]$, where T is the embedding class.

In view of the classification of the linear isomorphism class, this reduces the classification of symmetric models of a given degree d to the finite set of points T in $E[2]$ (and more precisely, for models over k, to T in $E[2](k)$).

Linear action of torsion

To complete the analysis of models up to linear equivalence, we finally recall a classification of linear translation maps.

Theorem

Let E be a projective degree d model of an elliptic curve, determined by a complete linear system. Then the translation-by-T morphism τ_T acts linearly if and only if T is in $E[d]$.

The statement is geometric — it is sufficient that T in $E(\bar{k})$, but T and τ_T have common fields of definition. This gives an argument for studying elliptic curve models in $\mathbb{P}^r$, for $r = d - 1$, together with a rational d-torsion structure. Of particular interest are cubic models with a 3-torsion structure e.g. $X^3 + Y^3 + Z^3 = cXYZ$, or a quartic model with 4-level structure.

Notions of complexity

We first recall some notation for the complexity, which we use to estimate the cost of arithmetic on elliptic curves: **M** and **S** will denote the cost of a field multiplication and squaring, respectively, and **m** denotes the cost of multiplication by a fixed constant.

For a finite field of q elements, typical algorithms for multiplication take time in $O(\log(q)^\omega)$ for some $1 + \varepsilon \leq \omega \leq 2$, with a possibly better constant for squaring. A naive implementation gives the upper bound, Karatsuba gives an $\omega = \log_2(3)$ algorithm, and fast Fourier transform provides an asymptotic complexity of $1 + \varepsilon$.

We ignore additions, which lie in the class $O(\log(q))$, and distinguish multiplication by a constant, which, for fixed small size or sparse values, can reduce to $O(\log(q))$.

Evaluating isogenies

In order to minimize the number of arithmetic operations, it is important to control the degree of the defining polynomials for an isogeny.

Theorem

An isogeny $\phi : E_1 \to E_2$ of degree n, between models given by complete linear systems of degree d, is given by polynomials of degree n if and only if

- $\phi^* \mathscr{L}_2 \cong \mathscr{L}_1^n$, *where* $\mathscr{L}_i$ *are the embedding sheaves,*
- $\phi^*(H_2 \cap E_2) \sim n \cdot H_1 \cap E_1$ *for any hyperplanes* H_2 *and* H_1,
- *the embedding classes* T_1 *and* T_2 *satisfy*

$$n(T_1 - S_1) = d \sum_{Q \in G} Q \text{ where } S_1 \in \phi^{-1}(T_2) \text{ and } G = \ker(\phi).$$

If it exists, a tuple $(f_0, \ldots, f_r)$ of polynomials of degree n defining ϕ is unique in $k[E_1]^d$ up to a scalar multiple.

Evaluating isogenies

As a consequence, the full multiplication-by-n maps behave well.

Corollary

The multiplication-by-n map on any symmetric projective model is uniquely determined by polynomials of degree n^2.

This contrasts with the curious fact that 2-isogenies are not well-suited to elliptic curves in Weierstrass form.

Corollary

There does not exist a cyclic isogeny of even degree n given by polynomials of degree n between curves in Weierstrass form.

Evaluating isogenies

Example. Let $E : Y^2Z = X(X^2 + aXZ + bZ^2)$ be an elliptic curve with rational 2-torsion point $(0 : 0 : 1)$. The quotient by $G = \langle (0 : 0 : 1) \rangle$, to the curve $Y^2Z = X((X - aZ)^2 - 4bZ^2)$, is given by a 3-dimensional space of polynomial maps of degree 3:

$$(X : Y : Z) \longmapsto$$
$$\begin{cases} (Y^2Z : (X^2 - bZ^2)Y : X^2Z) \\ ((X + aZ)Y^2 : (Y^2 - 2bXZ - abZ^2)Y : X^2(X + aZ)) \\ ((X^2 + aXZ + bZ^2)Y : XY^2 - b(X^2 + aXZ + bZ^2)Z : XYZ) \end{cases}$$

but not by any system of polynomials of degree 2.

Efficient scalar multiplication

The principle focus for efficient arithmetic is the operation of scalar multiplication by k. Using a standard windowing technique, we write $k = \sum_{i=0}^{t} a_i n^i$ in base $n = \ell^k$ (the window), and precompute $[a_i](P)$ for a_i in $(\mathbb{Z}/n\mathbb{Z})^*$. We may then compute $[k](P)$, using t additions and kt scalings by $[\ell]$.

In order to break down the problem further, we suppose the existence of an isogeny decomposition $[\ell] = \hat{\phi}\phi$, for which we need a rational cyclic subgroup $G \subset E[n]$ (where in practise $n = \ell = 3$ or $n = \ell^2 = 4$ — the window may be a higher power of ℓ). For this purpose we study families of elliptic curves with G-level structure.

In view of the analysis of torsion action and degrees of defining polynomials, we give preference to degree d models where $n \mid d$, and G will be either $\mathbb{Z}/n\mathbb{Z}$ or $\boldsymbol{\mu}_n$ (as a group scheme).

Strategy for efficient isogeny computation

Suppose we are given E_1 and E_2 in $\mathbb{P}^r$ with isogeny $\phi : E_1 \to E_2$ given by defining polynomials $(f_0, \ldots, f_r)$ of degree $n = \deg(\phi)$.

The computational strategy is the following: we set

$$V_0 = \Gamma(\mathbb{P}^r, \mathscr{I}_E(n)) = \ker\left(\Gamma(\mathbb{P}^r, \mathcal{O}(n)) \to \Gamma(E, \mathscr{L}^n)\right),$$

and successively construct a flag

$$V_0 \subset V_1 \subset \cdots \subset V_d = V_0 + \langle f_0, \ldots, f_d \rangle$$

such that each space V_{i+1} is constructed by adjoining to V_i a form $g_i \in (V_0 + \langle f_0, \ldots, f_d \rangle) \backslash V_i$, minimizing the number of **M** and **S**.

Subsequently the forms $f_0, \ldots, f_r$ can be expressed in terms of the generators $g_0, \ldots, g_r$ with complexity $O(\mathbf{m})$, with retrospective optimization of the constant multiplications.

Arithmetic on cubic models

For optimization of arithmetic on a cubic family we consider a univeral curve with $\boldsymbol{\mu}_3$ level structure, the *twisted Hessian normal form*:

$$H : aX^3 + Y^3 + Z^3 = XYZ,\ O = (0 : 1 : -1),$$

obtained by descent of the Hessian model $X^3 + Y^3 + Z^3 = cXYZ$ to $a = c^3$, by coordinate scaling (cf. Bernstein-K-Lange). Addition on this model is reasonably efficient at a cost of $12\mathbf{M}$. In order to optimize the tripling morphism [3], we consider the quotient by $\boldsymbol{\mu}_3 = \langle(0 : \omega : -1)\rangle$.

By means of the isogeny $(X : Y : Z) \mapsto (aX^3 : Y^3 : Z^3)$, with kernel $\boldsymbol{\mu}_3$, we obtain the quotient elliptic curve

$$E : XYZ = a(X + Y + Z)^3,\ O = (0 : 1 : -1).$$

This yields an isogeny ϕ of cubic models by construction, at a cost of three cubings: $3\mathbf{M} + 3\mathbf{S}$.

Arithmetic on cubic models

In the previous construction, by using the $\boldsymbol{\mu}_n$ structure, with respect to which the coordinate functions are diagonalized, we were able to construct the quotient isogeny

$$(X_0 : \cdots : X_r) \mapsto (X_0^n : \cdots : X_r^n)$$

without much effort. In remains to construct the dual.

In the case of the twisted Hessian, the dual isogeny $\psi = \hat{\phi}$ is given by $(X : Y : Z) \mapsto (f_0 : f_1 : f_2)$, where

$$\begin{aligned} f_0 &= X^3 + Y^3 + Z^3 - 3XYZ, \\ f_1 &= X^2Y + Y^2Z + XZ^2 - 3XYZ, \\ f_2 &= XY^2 + YZ^2 + X^2Z - 3XYZ \end{aligned}$$

as we can compute by pushing [3] through ϕ.

Arithmetic on cubic models

The quotient curve $E : XYZ = a(X + Y + Z)^3$, admits a $\mathbb{Z}/3\mathbb{Z}$-level structure, acting by cyclic coordinate permutation. The isogeny $\psi : E \to H$ is the quotient of this group $G = \ker(\psi)$ must be defined by polynomials in

$$\Gamma(E, \mathscr{L}_E^3)^G = \langle X^3+Y^3+Z^3, X^2Y+Y^2Z+XZ^2, XY^2+YZ^2+X^2Z \rangle$$

modulo the relation $XYZ = a(X + Y + Z)^3$. We note, however, that the map $\psi^* : \Gamma(H, \mathscr{L}_H) \to \Gamma(E, \mathscr{L}_E^3)^G$ must be surjective since both have dimension 3.

Using the group action, we construct the norm map

$$N_G : \Gamma(E, \mathscr{L}) \to \Gamma(E, \mathscr{L}_E^3)^G,$$

by $N_G(f) = f(X, Y, Z)f(Y, Z, X)f(Z, X, Y)$. It is nonlinear but sufficient to provides a set of generators using $1\mathbf{M} + 1\mathbf{S}$ each.

Arithmetic on cubic models

As a first norm we take $g_0 = N_G(X+Y+Z) = (X+Y+Z)^3$, then note that $N_G(X) = N_G(Y) + N_G(Z) = XYZ = ag_0$. It remains to complete a basis with, for example,

$$g_1 = N_G(Y+Z) = (Y+Z)(X+Z)(X+Y),$$
$$g_2 = N_G(Y-Z) = (Y-Z)(Z-X)(X-Y),$$

then to find the linear transformation

$$f_0 = (1-3a)g_0 - 3g_1,$$
$$f_1 = -4ag_0 + (g_1 - g_2)/2,$$
$$f_2 = -4ag_0 + (g_1 + g_2)/2.$$

This gives an algorithm for ψ using $5\mathbf{M} + 1\mathbf{S}$, for a total complexity for tripling ($[3] = \psi \circ \phi$) of $8\mathbf{M} + 4\mathbf{S}$. Attributing $1\mathbf{m}$ for the multiplications by a, ignoring additions implicit in the small integers (after scaling by 2), this gives $8\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$.

Arithmetic on cubic models

Is this interesting?

- Previous algorithms required $8\mathbf{M} + 6\mathbf{S} + 1\mathbf{m}$.
- A comparison with doubling should scale by $\log_3(2)$.
- Fast doublings exist for
  - Singular Edwards models in $\mathbb{P}^2$, using $3\mathbf{M} + 4\mathbf{S}$.
  - Extended Edwards models in $\mathbb{P}^3$, using $4\mathbf{M} + 4\mathbf{S}$.

This leads to the following complexities of $[\ell]$ and addition $\oplus$:

	Cost of $1\mathbf{S}$			
$[\ell]$	$1.00\mathbf{M}$	$0.80\mathbf{M}$	$0.67\mathbf{M}$	$\oplus$
$4\mathbf{M} + 4\mathbf{S}$	$8.00\mathbf{M}$	$7.20\mathbf{M}$	$6.67\mathbf{M}$	$9\mathbf{M}$
$(8\mathbf{M} + 4\mathbf{S})\log_3(2)$	$7.57\mathbf{M}$	$7.07\mathbf{M}$	$6.73\mathbf{M}$	$12\mathbf{M}\log_3(2) = 7.57\mathbf{M}$
$3\mathbf{M} + 4\mathbf{S}$	$7.0\mathbf{M}$	$6.20\mathbf{M}$	$5.67\mathbf{M}$	$11\mathbf{M}$

This analysis brings tripling in line with with doubling (on optimal models for each) for use in scalar multiplication in cryptography. The method of analysis reduces the discovery of efficient arithmetic to hand computation. THE END

Arithmetic on cubic models

Is this interesting?

- Previous algorithms required $8\mathbf{M} + 6\mathbf{S} + 1\mathbf{m}$.
- A comparison with doubling should scale by $\log_3(2)$.
- Fast doublings exist for
  - Singular Edwards models in $\mathbb{P}^2$, using $3\mathbf{M} + 4\mathbf{S}$.
  - Extended Edwards models in $\mathbb{P}^3$, using $4\mathbf{M} + 4\mathbf{S}$.

This leads to the following complexities of $[\ell]$ and addition $\oplus$:

	Cost of $1\mathbf{S}$			
$[\ell]$	$1.00\mathbf{M}$	$0.80\mathbf{M}$	$0.67\mathbf{M}$	$\oplus$
$4\mathbf{M} + 4\mathbf{S}$	$8.00\mathbf{M}$	$7.20\mathbf{M}$	$6.67\mathbf{M}$	$9\mathbf{M}$
$(8\mathbf{M} + 4\mathbf{S})\log_3(2)$	$7.57\mathbf{M}$	$7.07\mathbf{M}$	$6.73\mathbf{M}$	$12\mathbf{M}\log_3(2) = 7.57\mathbf{M}$
$3\mathbf{M} + 4\mathbf{S}$	$7.0\mathbf{M}$	$6.20\mathbf{M}$	$5.67\mathbf{M}$	$11\mathbf{M}$

This analysis brings tripling in line with with doubling (on optimal models for each) for use in scalar multiplication in cryptography. The method of analysis reduces the discovery of efficient arithmetic to hand computation. **THE END**