About the CRT method to compute class polynomials in dimension 2

Journées C2

Kristin Lauter[1], **Damien Robert**[2]

[1]Microsoft Research [2]LFANT Team, IMB & INRIA Bordeaux Sud-Ouest

05/04/2011 (Oléron)

Motivation

Abelian varieties and cryptography

If $A/\mathbb{F}_q$ is a “generic” abelian variety of small dimension g, then the DLP on $A(\mathbb{F}_q)$ is thought to be hard if $\#A(\mathbb{F}_q)$ is divisible by a large prime.

- Take random abelian varieties and count the number of points (a bit too slow when $g=2$);
- Generate abelian varieties with a prescribed number of points ($\Rightarrow$ paring based cryptography).

Class polynomials

- If $A/\mathbb{F}_q$ is an ordinary (simple) abelian variety of dimension g, $\mathrm{End}(A) \otimes \mathbb{Q}$ is a (primitive) CM field K (K is a totally imaginary quadratic extension of a totally real number field K_0).
- The class polynomials $H_1, \ldots, H_{g(g+1)/2}$ parametrizes the invariants of all abelian varieties $A/\mathbb{C}$ with $\mathrm{End}(A) \simeq O_K$.
- If the class polynomials are totally split modulo $\mathfrak{P}$, their roots in $\mathbb{F}_{\mathfrak{P}}$ gives invariants of abelian varieties $A/\mathbb{F}_{\mathfrak{P}}$ with $\mathrm{End}(A) \simeq O_K$. It is easy to recover $\#A(\mathbb{F}_{\mathfrak{P}})$ given O_K and $\mathfrak{P}$.

Some technical details

- The abelian varieties are principally polarized.
- A CM type Φ is a choice of an extension to K for each of the embedding $K_0 \to \mathbb{R}$. We have

$$\mathrm{Hom}(K,\mathbb{C}) = \Phi \oplus \overline{\Phi}.$$

- The isogeny class of complex abelian varieties with CM by K is determined by the class of Φ.
- The reflex field of (K,φ) is the CM field K^r generated by the traces $\sum_{\varphi\in\Phi}\varphi(x)$, $x\in K$.
- The type norm $N_\varphi : K \to K^r$ is $x \mapsto \prod_{\varphi\in\Phi}\varphi(x)$.

Theorem (Main theorems of complex multiplication)

- *The class polynomials $(H_\Phi)_i$ are defined over K_0 and generate a subfield $\mathfrak{H}_\Phi$ of the Hilbert class field of K^r.*
- *If $A/\mathbb{C}$ has CM by (O_K,Φ) and $\mathfrak{P}$ is a prime of good reduction in $\mathfrak{H}_\Phi$, then the Frobenius of $A_\mathfrak{P}$ corresponds to $N_{\mathfrak{H}_\Phi,\Phi^r}(\mathfrak{P})$.*

Constructing class polynomials

If $g \leqslant 2$, the CM types are in the same orbits under the absolute Galois action, and the class polynomials $H_i = \prod (H_\Phi)_i$ are rational (and even integral when $g = 1$).

- Analytic method: compute the invariants in $\mathbb{C}$ with sufficient precision to recover the class polynomials.
- p-adic lifting: lift the invariants in $\mathbb{Q}_p$ with sufficient precision to recover the class polynomials (require specific splitting behavior of p).
- CRT: compute the class polynomials modulo small primes, and use the CRT to reconstruct the class polynomials.

Remark

In genus 1, all these methods are quasi-linear in the size of the output $\Rightarrow$ computation bounded by memory. But we can construct directly the class polynomials modulo p with the explicit CRT.

Review of the CRT algorithm

To simplify, we assume here that K is a quartic Galois CM field (so $\mathrm{Gal}(K) = \mathbb{Z}/4\mathbb{Z}$ and there is only one CM type class).

1. Select a prime p.
2. For each abelian surface A in the p^3 isomorphic classes:
   - 2.1 Check if A is in the right isogeny class by computing the characteristic polynomial of the Frobenius (do some trial tests to check for $\#A$ before).
   - 2.2 Check if $\mathrm{End}(A) = O_K$.
3. From the invariants of the maximal curves, reconstruct H_i mod p.

Repeat until we can recover H_i from the $H_i \mod p$ using the CRT.

Remark

Since K is primitive, we only need to look at Jacobians of hyperelliptic curves of genus 2.

Selecting the prime p

- Usual method: find a prime p that splits completely into principal ideals in K^r, and splits completely in K.
- But we only need the typenorm of the ideals in K^r above p to be principal ideals.

⇒ We can work with more prime!

⇒ The typenorm give the frobenius.

Checking if a curve is maximal

- Let J be the Jacobian of a curve in the right isogeny class. Then $\mathbb{Z}[\pi,\overline{\pi}] \subset \mathrm{End}(J) \subset O_K$.
- Let $\gamma \in O_K \backslash \mathbb{Z}[\pi,\overline{\pi}]$. We want to check if $\gamma \in \mathrm{End}(J)$.
- Suppose that $(O_K : \mathbb{Z}[\pi,\overline{\pi}])$ is prime to p. We then have $\gamma \in \mathrm{End}(J) \Leftrightarrow p\gamma \in \mathrm{End}(J)$.
- Let n be the smallest integer thus that $n\gamma \in \mathbb{Z}[\pi,\overline{\pi}]$. Since $(\mathbb{Z}[\pi,\overline{\pi}] : \mathbb{Z}[\pi]) = p$, we can write $np\gamma = P(\pi)$.
- Then $\gamma \in \mathrm{End}(J) \Leftrightarrow P(\pi) = 0$ on $J[n]$.
- In practice (Freeman-Lauter): compute $J[\ell^d]$ for $\ell^d \mid (O_K : \mathbb{Z}[\pi,\overline{\pi}])$ and check the action of the generators of O_K on it.

Remark

If $1, \alpha, \beta, \gamma$ are generators of O_K as a $\mathbb{Z}$-module, it can happen that $\gamma = P(\alpha, \beta)$, so that we don't need to check that $\gamma \in \mathrm{End}(J)$.

Example 1: Checking if a curve is maximal

- Let $H : y^2 = 10x^6 + 57x^5 + 18x^4 + 11x^3 + 38x^2 + 12x + 31$ over $\mathbb{F}_{59}$ and J the Jacobian of H. We have $\mathrm{End}(J) \otimes \mathbb{Q} = \mathbb{Q}(i\sqrt{29 + 2\sqrt{29}})$ and we want to check if $\mathrm{End}(J) = O_K$.
- O_K is generated as a $\mathbb{Z}$-module by $1, \alpha, \beta, \gamma$. α is of index 2 in $O_K/\mathbb{Z}[\pi, \overline{\pi}]$, β of index 4 and γ of index 40.
- So the old algorithm will check $J[2^3]$ and $J[5]$.
- But $(O_K)_2 = \mathbb{Z}_2[\pi, \overline{\pi}, \alpha]$, so we only need to check $J[2]$ and $J[5]$.

Computing the ℓ^d-torsion

- We compute $\#J(\mathbb{F}_{p^\alpha}) = \ell^\beta c$ (where α is the degree of definition of the ℓ^d-torsion).
- If P_0 is a random point of $J(\mathbb{F}_{p^\alpha})$, then $P = cP_0$ is a random point of ℓ^∞-torsion, and P multiplied by a suitable power of ℓ is a random point of ℓ^d-torsion.
- Usual method (Freeman-Lauter): take a lot of random points of ℓ^d-torsion, and hope they generate it over $\mathbb{F}_{p^\alpha}$.
- Problems: the random points of ℓ^d-torsion are not uniform $\Rightarrow$ require a lot of random points, and the result is probabilistic.
- Our solution: Compute the whole ℓ^∞-torsion. "Correct" points to find uniform points of ℓ^d-torsion. Use pairings to save memory.

$\Rightarrow$ We can check if a curve is maximal faster.

$\Rightarrow$ We can abort early.

Example 2: checking if a curve is maximal

- Let $H : y^2 = 80x^6 + 51x^5 + 49x^4 + 3x^3 + 34x^2 + 40x + 12$ over $\mathbb{F}_{139}$ and J the Jacobian of H. We have $\mathrm{End}(J) \otimes \mathbb{Q} = \mathbb{Q}(i\sqrt{13 + 2\sqrt{29}})$ and we want to check if $\mathrm{End}(J) = O_K$.
- For that we need to compute $J[3^5]$, that lives over an extension of degree 81 (for the twist it lives over an extension of degree 162).
- With the old randomized algorithm, this computation takes 470 seconds (with 12 Frobenius trials over $\mathbb{F}_{139^{162}}$).
- With the new algorithm computing the ℓ^∞-torsion, it only takes 17.3 seconds (needing only 4 random points over $\mathbb{F}_{139^{81}}$, approx 4 seconds needed to get a new random point of ℓ^∞-torsion).

Obtaining all the maximal curves

- If J is a maximal curve, and ℓ does not divide $(O_K : \mathbb{Z}[\pi, \overline{\pi}])$, then any (ℓ, ℓ)-isogenous curve is maximal.
- The maximal Jacobians form a principal homogeneous space under the Shimura class group $\mathfrak{C}(O_K) = \{(I, \rho) \mid I\overline{I} = (\rho) \text{ and } \rho \in K_0^+\}$.
- (ℓ, ℓ)-isogenies between maximal Jacobians correspond to element of the form $(I, \ell) \in \mathfrak{C}(O_K)$. We can use the structure of $\mathfrak{C}(O_K)$ to determine the number of new curves we will obtain with (ℓ, ℓ)-isogenies.
  $\Rightarrow$ Don't compute unneeded isogenies.
- It can be faster to compute (ℓ, ℓ)-isogenies with $\ell \mid (O_K : \mathbb{Z}[\pi, \overline{\pi}])$ to find new maximal Jacobians when ℓ and $\mathrm{val}_\ell((O_K : \mathbb{Z}[\pi, \overline{\pi}]))$ is small.

A little (and instructive!) publicity

But how to compute isogenies in dimension 2?

With AVIsogenies (Abelian varieties and isogenies) a powerful, efficient, fast and bug free (someday) Magma package for the algorithmic of abelian varieties!

You can find it with all good browsers on `http://avisogenies.gforge.inria.fr`.

Developed by Bisson , Cosset and R using results from Faugère Lubicz and R; Lubicz and R; Cosset and R.

"Going up"

- There is p^3 classes of isomorphic curves, but only a very small number $(\#\mathfrak{C}(O_K))$ with $\mathrm{End}(J) = O_K$.
- But there is at most $16p^{3/2}$ isogeny class.

$\Rightarrow$ On average, there is $\approx p^{3/2}$ curves in a given isogeny class.

$\Rightarrow$ If we have a curve in the right isogeny class, try to find isogenies giving a maximal curve!

An algorithm for "going up"

1. Let $\gamma \in O_K \setminus \mathrm{End}(J)$. We can assume that $\ell^\infty \gamma \in \mathbb{Z}[\pi, \overline{\pi}]$.
2. Let d be the minimum such that $\gamma(J[\ell^d]) \neq \{0\}$, and let $K = \gamma(J[\ell^d])$. By definition, $K \subset J[\ell]$.
3. We compute all (ℓ,ℓ)-isogeneous Jacobians J' where the kernel intersect K. Keep J' if $\#\gamma(J'[\ell^d]) < \#K$ (and be careful to prevent cycles).

- First go up for $\gamma = (\pi^\alpha - 1)/\ell$: this minimize the extensions we have to work with.
- It is not always possible to go up. We would need more general isogenies than (ℓ,ℓ)-isogenies. Most frequent case: we can't go up because there is no (ℓ,ℓ)-isogenies at all! (And we can detect this).

The modified CRT algorithm

1. Select a prime p.
2. Select a random Jacobian until it is in the right isogeny class.
3. Go up to find a Jacobian with CM by O_K (if it fails, go back to last step).
4. Use isogenies to find all other Jacobians with CM by O_K.
5. From the invariants of the maximal abelian surfaces, reconstruct $H_i \mod p$.

Remark

- *For the random search we use curves in Weierstrass form*

$$y^2 = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

If the two torsion is rational (check where $\frac{\pi-1}{2}$ *live), we can construct curves in Rosenhain form*

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu).$$

- *We sieve the primes (dynamically) by estimating the number of curves in the isogeny class.*

The dihedral case

- There are two CM types.
- A prime p which is nice for one CM type may be bad for the other. But we can't distinguish the CM types over $\mathbb{Q}$.
- However we can work over K_0, if $p = q_1 q_2$ in K_0, then one CM type correspond to the reduction modulo a prime in the class field above q_1, and the other to a prime above q_2. By doing the CRT on q_i, we keep track of this CM type.

⇒ This mean we can choose the "best" CM type!

- The class polynomials over K_0 splits into polynomials given by the action of the type norm. It is easy to compute the orbits modulo p, we can paste them using the "trace trick" from Enge and Sutherland.

Example

- K is the CM field defined by X^4+13X^2+41. $O_{K_0}=\mathbb{Z}[\alpha]$ where α is a root of $X^2-3534X+177505$.
- The class polynomials are (using absolute Igusa invariants given in Streng's thesis):

$$H_1=256X-2030994+56133\alpha;$$
$$H_2=128X+12637944-2224908\alpha;$$
$$H_3=65536X-11920680322632+1305660546324\alpha.$$

- Primes used: 59, 139, 241, 269, 131, 409, 541, 271, 359, 599, 661, 761.
- Denominators: use a bound or do a rational reconstruction in K_0 with LLL.

A pessimal view on the complexity of the CRT method in dimension 2

$\Delta_1 = \Delta_{K_0/\mathbb{Q}}$, $\Delta_0 = N_{K_0/\mathbb{Q}}(\Delta_{K/K_0}$.

- The degree of the class polynomials is $\widetilde{O}(\Delta_0^{1/2}\Delta_1^{1/2})$.
- The size of coefficients is bounded by $\widetilde{O}(\Delta_0^{5/2}\Delta_1^{3/2})$ (non optimal). In practice, they are $\widetilde{O}(\Delta_0^{1/2}\Delta_1^{1/2})$.

$\Rightarrow$ The size of the class polynomials is $\widetilde{O}(\Delta_0\Delta_1)$.

- We need $\widetilde{O}(\Delta_0^{1/2}\Delta_1^{1/2})$ primes, and by Cebotarev the density of primes we can use is $\widetilde{O}(\Delta_0^{1/2}\Delta_1^{1/2}) \Rightarrow$ the largest prime is $p = \widetilde{O}(\Delta_0\Delta_1)$.

$\Rightarrow$ Finding a curve in the right isogeny class will take $\Omega(p^{3/2})$ so the total complexity is $\Omega(\Delta_0^2\Delta_1^2) \Rightarrow$ we can't achieve quasi-linearity!

$\Rightarrow$ A solution would be to work over convenient subspaces of the moduli space.