

# Improved CRT Algorithm for class polynomials in genus 2

ANTS X

Kristin Lauter<sup>1</sup>, **Damien Robert**<sup>2</sup>

<sup>1</sup>Microsoft Research <sup>2</sup>LFANT Team, INRIA Bordeaux Sud-Ouest

09/07/2012 (San Diego)

# Class polynomials

- If  $A/\mathbb{F}_q$  is an ordinary (simple) abelian variety of dimension  $g$ ,  $\text{End}(A) \otimes \mathbb{Q}$  is a (primitive) CM field  $K$  ( $K$  is a totally imaginary quadratic extension of a totally real number field  $K_0$ ).
- The class polynomials  $H_1, \widehat{H}_2, \dots, \widehat{H}_{g(g+1)/2}$  parametrizes the invariants of all abelian varieties  $A/\mathbb{C}$  with  $\text{End}(A) \simeq O_K$ .
- 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  $\text{End}(A) \simeq O_K$ . 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  $\Phi$  is a choice of an extension to  $K$  for each of the embedding  $K_0 \rightarrow \mathbb{R}$ . We have

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

**Example:** If  $K$  is a (primitive) CM field of degree 4, then either  $K$  is cyclic and there is one class of CM type, or  $K$  is dihedral and there is two class of CM types.

- If  $A$  is an abelian variety with CM by  $K$ , the representation  $K \rightarrow \mathrm{End} T_0 A$  is given by a CM type  $\Phi$  (which determines the isogeny class of  $A$ ).
- The reflex field of  $(K, \varphi)$  is the CM field  $K^r$  generated by the traces  $\sum_{\varphi \in \Phi} \varphi(x)$ ,  $x \in K$ .
- The type norm  $N_\Phi: K \rightarrow K^r$  is  $x \mapsto \prod_{\varphi \in \Phi} \varphi(x)$ .

## Definition

The class polynomials  $(H_{\Phi, i})$  parametrizes the abelian varieties with CM by  $(O_K, \Phi)$

# Class polynomials and complex multiplication

## Theorem (Main theorems of complex multiplication)

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

If  $g \leq 2$ , the CM types are in the same orbits under the absolute Galois action, and the class polynomials  $H_i = \prod_{\Phi} H_{\Phi,i}$  are rationals (and even integrals when  $g = 1$ ).

- For efficiency, we compute the class polynomials  $H_{\Phi}$  since they give a factor of the full class polynomials  $H$ . This means we need less precision.
- In genus 2, this involves working over  $K_0$  rather than  $\mathbb{Q}$  in the Dihedral case.

# Constructing class polynomials

- 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 in genus 2

- 1 Select a CRT prime  $p$ .
- 2 For each abelian surface  $A$  in the  $O(p^3)$  isomorphic classes:
  - 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 Check if  $\text{End}(A) = O_K$ .
- 3 From the invariants of the maximal curves, reconstruct  $H_{\Phi,i} \pmod p$ .

Repeat until we can recover  $(H_{\Phi,i})$  from the  $(H_{\Phi,i} \pmod p)$  using the CRT.

## Remark

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

# Selecting the prime $p$

## Definition

A CRT prime  $\mathfrak{p} \subset O_{K_0^r}$  is a prime such that all abelian varieties over  $\mathbb{C}$  with CM by  $(O_K, \Phi)$  have good reduction modulo  $\mathfrak{p}$ .

- $\mathfrak{p}$  is a CRT prime for the CM type  $\Phi$  if and only if there exists an unramified prime  $q$  in  $O_{K^r}$  of degree 1 above  $p$  of principal type norm  $(\pi)$
  - The isogeny class of the reduction of these abelian varieties mod  $\mathfrak{p}$  is determined (up to a twist) by  $\pm\pi$  where  $N_{\Phi}(\mathfrak{p}) = (\pi)$ .
  - For efficiency, we work with CRT primes  $\mathfrak{p}$  that are unramified of degree one over  $p = \mathfrak{p} \cap \mathbb{Z}$ .
- ⇒ the reduction to  $\mathbb{F}_p$  of the abelian varieties with CM by  $(O_K, \Phi)$  will then be ordinary.

# Checking if a curve is maximal

- Let  $J$  be the Jacobian of a curve in the right isogeny class. Then  $\mathbb{Z}[\pi, \bar{\pi}] \subset \text{End}(J) \subset O_K$ .
- Let  $\gamma \in O_K \setminus \mathbb{Z}[\pi, \bar{\pi}]$ . We want to check if  $\gamma \in \text{End}(J)$ .
- If  $p > 3$  then  $(O_K : \mathbb{Z}[\pi, \bar{\pi}])$  is prime to  $p$ . We then have  $\gamma \in \text{End}(J) \Leftrightarrow p\gamma \in \text{End}(J)$ .
- Let  $n$  be the smallest integer thus that  $n\gamma \in \mathbb{Z}[\pi, \bar{\pi}]$ . Since  $(\mathbb{Z}[\pi, \bar{\pi}] : \mathbb{Z}[\pi]) = p$ , we can write  $np\gamma = P(\pi)$ .
- Then  $\gamma \in \text{End}(J) \Leftrightarrow P(\pi) = 0$  on  $J[n]$ .
- In practice (Freeman-Lauter): compute  $J[\ell^d]$  for  $\ell^d \mid (O_K : \mathbb{Z}[\pi, \bar{\pi}])$  and check the action of the generators of  $O_K$  on it.
- Our method: faster computation of  $J[\ell^d]$  using parings.

## 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  $\gamma \in \text{End}(J)$ .*



# 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  $\text{End}(J) \otimes \mathbb{Q} = \mathbb{Q}(i\sqrt{29 + 2\sqrt{29}})$  and we want to check if  $\text{End}(J) = O_K$ .
- $O_K$  is generated as a  $\mathbb{Z}$ -module by  $1, \alpha, \beta, \gamma$ .  $\alpha$  is of index 2 in  $O_K/\mathbb{Z}[\pi, \bar{\pi}]$ ,  $\beta$  of index 4 and  $\gamma$  of index 40.
- So the old algorithm will check  $J[2^3]$  and  $J[5]$ .
- But  $(O_K)_2 = \mathbb{Z}_2[\pi, \bar{\pi}, \alpha]$ , so we only need to check  $J[2]$  and  $J[5]$ .

## 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  $\text{End}(J) \otimes \mathbb{Q} = \mathbb{Q}(i\sqrt{13+2\sqrt{29}})$  and we want to check if  $\text{End}(J) = O_K$ .
- 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  $\ell^\infty$ -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  $\ell^\infty$ -torsion).

# Obtaining all the maximal curves

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

# “Going up”

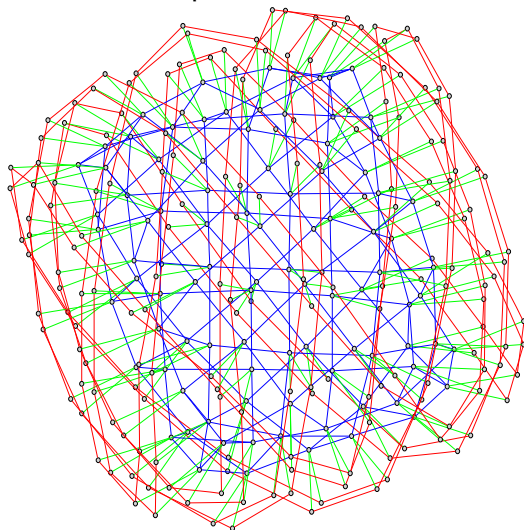
- There is  $p^3$  classes of isomorphic curves, but only a very small number ( $\#\mathcal{C}(O_K)$ ) with  $\text{End}(J) = O_K$ .
  - But there is at most  $16p^{3/2}$  isogeny class.
- ⇒ On average, there is  $\approx p^{3/2}$  curves in a given isogeny class.
- ⇒ If we have a curve in the right isogeny class, try to find isogenies giving a maximal curve!

# An algorithm for “going up”

- 1 Let  $\gamma \in O_K \setminus \text{End}(J)$ . We can assume that  $\ell^\infty \gamma \in \mathbb{Z}[\pi, \bar{\pi}]$ .
- 2 Let  $d$  be the smallest integer 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  $(\ell, \ell)$ -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.

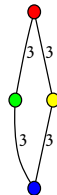
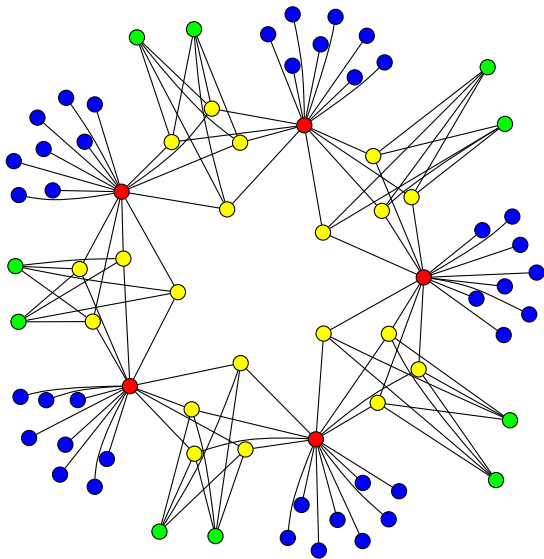
# Some pesky details

Non maximal cycles  $\Rightarrow$  We try to reduce globally the obstruction for all endomorphisms.



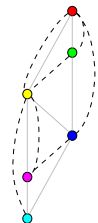
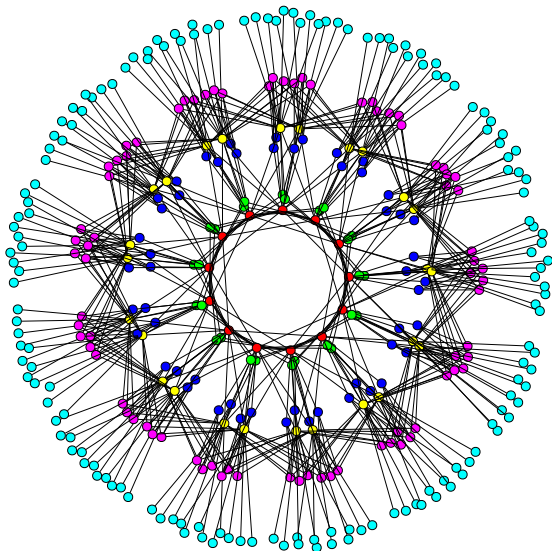
# Some pesky details

## Local minimums I



# Some pesky details

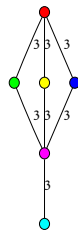
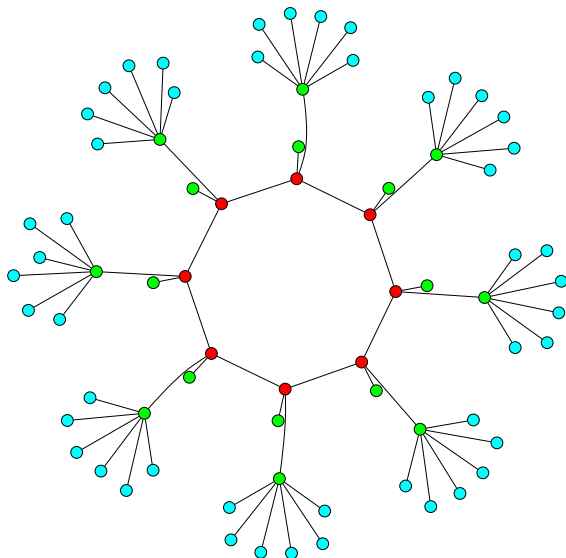
## Local minimums II





# Some pesky details

## Polarizations



# Some pesky details

- It is not always possible to go up. We would need more general isogenies than  $(\ell, \ell)$ -isogenies.
- Most frequent case: we can't go up because there is no  $(\ell, \ell)$ -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  $H_i \bmod p$ .

## Further details

- We sieve the primes  $p$  (using a dynamic approach).
- Estimate the number of curves where we can go up as

$$\sum_{d|[O_K:\mathbb{Z}[\pi,\bar{\pi}]]} \#\mathfrak{C}(\mathbb{Z}[\pi,\bar{\pi}])/d$$

(for  $[O_K:\mathbb{Z}[\pi,\bar{\pi}]]/d$  not divisible by a  $\ell$  where we can't go up),  
with

$$\#\mathfrak{C}(\mathbb{Z}[\pi,\bar{\pi}]) = \frac{c(O_K:\mathbb{Z}[\pi,\bar{\pi}])\#\text{Cl}(O_K)\text{Reg}(O_K)(\widehat{O}_K^*:\widehat{\mathbb{Z}}[\pi,\bar{\pi}]^*)}{2\#\text{Cl}(\mathbb{Z}[\pi+\bar{\pi}])\text{Reg}(\mathbb{Z}[\pi+\bar{\pi}])}$$

- To find the denominators: do a rational reconstruction in  $K_0^r$  using LLL or use Brunier-Yang formulas.

$p$	$l^d$	$\alpha_d$	# Curves	Estimate	Time (old)	Time (new)
7	$2^2$	4	7	8	0.5+0.3	0+0.2
17	2	1	39	32	4+0.2	0+0.1
23	$2^2, 7$	4, 3	49	51	9+2.3	0+0.2
71	$2^2$	4	7	8	255+0.7	5.3+0.2
97	2	1	39	32	680+0.3	2+0.1
103	$2^2, 17$	4, 16	119	127	829+17.6	0.5+1
113	$2^5, 7$	16, 6	1281	877	1334+28.8	0.2+1.3
151	$2^2, 7, 17$	4, 3, 16	-	-	0	0
					3162s	13s

Computing the class polynomial for  $K = \mathbb{Q}(i\sqrt{2+\sqrt{2}})$ ,  $\mathfrak{C}(O_K) = \{0\}$ .

$$H_1 = X - 1836660096, \quad H_2 = X - 28343520, \quad H_3 = X - 9762768$$

$p$	$l^d$	$\alpha_d$	# Curves	Estimate	Time (old)	Time (new)
29	3,23	2,264	-	-	-	-
53	3,43	2,924	-	-	-	-
61	3	2	9	6	167+0.2	0.2+0.5
79	3 <sup>3</sup>	18	81	54	376+8.1	0.3+0.9
107	3 <sup>2</sup> ,43	6,308	-	-	-	-
113	3,53	1,52	159	155	1118+137.2	0.8+25
131	3 <sup>2</sup> ,53	6,52	477	477	1872+127.4	2.2+44.4
139	3 <sup>5</sup>	81	?	486	-	1+36.7
157	3 <sup>4</sup>	27	243	164	3147+16.5	-
					6969s	114s

Computing the class polynomial for  $K = \mathbb{Q}(i\sqrt{13+2\sqrt{29}})$ ,  $\mathfrak{C}(O_K) = \{0\}$ .

$$H_1 = X - 268435456, \quad H_2 = X + 5242880, \quad H_3 = X + 2015232.$$

$p$	$l^d$	$\alpha_d$	# Curves	Estimate	Time (old)	Time (new)
7	-	-	1	1	0.3	0+0.1
23	<b>13</b>	84	15	2 (16)	9+70.7	0.4+24.6
53	7	3	7	7	105+0.5	7.7+0.5
59	<b>2,5</b>	1,12	322	48 (286)	164+6.4	1.4+0.6
83	3,5	4,24	77	108	431+9.8	2.4+1.1
103	67	1122	-	-	-	-
107	<b>7,13</b>	3,21	105	8 (107)	963+69.3	-
139	<b>5<sup>2</sup>,7</b>	60,2	259	9 (260)	2189+62.1	-
181	3	1	161	135	5040+3.6	4.5+0.2
197	5,109	24,5940	-	-	-	-
199	<b>5<sup>2</sup></b>	60	37	2 (39)	10440+35.1	-
223	2,23	1,11	1058	39 (914)	10440+35.1	-
227	109	1485	-	-	-	-
233	5,7, <b>13</b>	8,3,28	735	55 (770)	11580+141.6	88.3+29.4
239	7,109	6,297	-	-	-	-
257	3,7, <b>13</b>	4,6,84	1155	109 (1521)	17160+382.8	-
313	<b>3,13</b>	1,14	?	146 (2035)	-	165+14.7
373	5,7	6,24	?	312	-	183.4+3.8
541	<b>2,7,13</b>	1,3,14	?	294 (4106)	-	91+5.5
571	<b>3,5,7</b>	2,6,6	?	1111 (6663)	-	96.6+3.1
					56585s	776s

Computing the class polynomial for  $K = \mathbb{Q}(i\sqrt{29+2\sqrt{29}})$ ,  $\mathfrak{C}(O_K) = \{0\}$ .

$$H_1 = 244140625X - 2614061544410821165056$$

# A Dihedral example

- $K$  is the CM field defined by  $X^4 + 13X^2 + 41$ .  $O_{K_0} = \mathbb{Z}[\alpha]$  where  $\alpha$  is a root of  $X^2 - 3534X + 177505$ .
- We first compute the class polynomials over  $\mathbb{Z}$  using Spallek's invariants, and obtain the following polynomials in 5956 seconds:

$$H_1 = 64X^2 + 14761305216X - 11157710083200000$$

$$H_2 = 16X^2 + 72590904X - 8609344200000$$

$$H_3 = 16X^2 + 28820286X - 303718531500$$

- Next we compute them over the real subfield and using Streng's invariants. We get in 1401 seconds:

$$H_1 = 256X - 2030994 + 56133\alpha;$$

$$H_2 = 128X + 12637944 - 2224908\alpha;$$

$$H_3 = 65536X - 11920680322632 + 1305660546324\alpha.$$

- Primes used: 59, 139, 241, 269, 131, 409, 541, 271, 359, 599, 661, 761.



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

- The degree of the class polynomials is  $\tilde{O}(\Delta_0^{1/2} \Delta_1^{1/2})$ .
  - The size of coefficients is bounded by  $\tilde{O}(\Delta_0^{5/2} \Delta_1^{3/2})$  (non optimal).  
In practice, they are  $\tilde{O}(\Delta_0^{1/2} \Delta_1^{1/2})$ .
- ⇒ The size of the class polynomials is  $\tilde{O}(\Delta_0 \Delta_1)$ .
- We need  $\tilde{O}(\Delta_0^{1/2} \Delta_1^{1/2})$  primes, and by Cebotarev the density of primes we can use is  $\tilde{O}(\Delta_0^{1/2} \Delta_1^{1/2}) \Rightarrow$  the largest prime is  $p = \tilde{O}(\Delta_0 \Delta_1)$ .
- ⇒ 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 even if the going-up step always succeed!
- ⇒ A solution would be to work over convenient subspaces of the moduli space.

# Perspectives

- In progress: Improve the search for curves in the isogeny class;
- In progress: combine the going-up method with Bisson's sub-exponential endomorphism ring computation. Particularly interesting when a power divides the index;
- Use Iovica pairing based approach to choose horizontal kernels in the maximal step;
- Change the polarization;
- Work inside Humbert surfaces;
- Work with supersingular abelian varieties;
- More general isogenies than  $(\ell, \ell)$ -isogenies.