Improved CRT Algorithm for class polynomials in genus 2

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

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

01/08/2012 (Microsoft Research)

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).
- Inverse problem: given a CM field K, construct the class polynomials $H_1, \widehat{H}_2 \dots, \widehat{H}_{g(g+1)/2}$ which parametrizes the invariants of all abelian varieties $A/\mathbb{C}$ with $\mathrm{End}(A) \simeq O_K$.
- Cryptographic application: if the class polynomials are totally split modulo an ideal $\mathfrak{P}$, 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.
- CM-types: a partition $\mathrm{Hom}(K,\mathbb{C}) = \Phi \oplus \overline{\Phi}$.
- In genus 2, the CM field K of degree 4 will be either cyclic (and Galoisian) or Dihedral (and non Galoisian). The latter case appear most often, and in this case we have two CM-types.

Definition

- The class polynomials $(H_{\Phi,i})$ parametrizes the abelian varieties with CM by (O_K, 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 $N_\Phi : K \to K^r$ is $x \mapsto \prod_{\varphi\in\Phi} \varphi(x)$.

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, Φ) and $\mathfrak{P}$ is a prime of good reduction in $\mathfrak{H}_\Phi$, then the Frobenius of $A_\mathfrak{P}$ corresponds to $N_{\mathfrak{H}_\Phi,\Phi^r}(\mathfrak{P})$.*

- For efficiency, we compute the class polynomials $H_{\Phi,i}$ since they give a factor of the full class polynomials H_i. This mean 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 so the CRT approach is only time dependent.*

Review of the CRT algorithm in genus 2

1. Select a CRT prime p;
2. Find all abelian surfaces $A/\mathbb{F}_p$ with CM by (O_K, Φ);
3. From the invariants of the maximal abelian surfaces, reconstruct $H_{\Phi,i} \mod p$.

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

Remark

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

Isogenies and endomorphism ring

- If $A/\mathbb{F}_p$ is an abelian surface, the CM field $K = \mathrm{End}(A) \otimes \mathbb{Q}$ is generated by the Frobenius π;
- If $A = \mathrm{Jac}(H)$ then the characteristic polynomial χ_π (and therefore K) is uniquely determined by $\#H$ and $\#A$;
- Tate: the isogeny class of A is given by all the other abelian surfaces with CM field K ("isogenous $\Leftrightarrow$ same number of points");
- The CM order $\mathrm{End}(A) \subset K$ is a finer invariant which partition the isogeny class (one subset for every order O such that $\mathbb{Z}[\pi, \overline{\pi}] \subset O \subset O_K$ and O is stable by the complex conjugation).

Definition

Les $f : A \to B$ be an isogeny. Then we call f horizontal if $\mathrm{End}(A) = \mathrm{End}(B)$. Otherwise we call f vertical.

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, Φ) have good reduction modulo $\mathfrak{p}$.

- $\mathfrak{p}$ is a CRT prime for the CM type Φ if and only if there exists an unramified prime $\mathfrak{q}$ in O_{K^r} of degree 1 above p of principal type norm (π);
- The isogeny class of the reduction of these abelian varieties mod $\mathfrak{p}$ is determined (up to a twist) by $\pm\pi$ where $N_\Phi(\mathfrak{p}) = (\pi)$.

Remark

For efficiency, we work with CRT primes $\mathfrak{p}$ that are unramified of degree one over $p = \mathfrak{p} \cap \mathbb{Z}$;

$\Rightarrow$ *the reduction to $\mathbb{F}_p$ of the abelian varieties with CM by (O_K, Φ) will then be ordinary.*

The case of elliptic curves

- Let K be an imaginary quadratic field of Discriminant Δ. Then H_{O_K} has degree $O(\sqrt{\Delta})$ with coefficients of size $\widetilde{O}(\sqrt{\Delta})$;
- The CRT step will use $\widetilde{O}(\sqrt{\Delta})$ primes p of size $\widetilde{O}(\Delta)$;
- For each CRT prime p there is $O(p)$ isomorphic classes of elliptic curves, $O(\sqrt{p})$ curves inside the isogeny class corresponding to K and $O(\sqrt{p})$ curves with $\mathrm{End}(E) = O_K$;

$\Rightarrow$ Finding a maximal curve takes time $O(\sqrt{p})$.

- Once a maximal curve is found, compute all the others using horizontal isogenies (very fast);

$\Rightarrow$ Finding all maximal curves take time $\widetilde{O}(\sqrt{p})$, for a total complexity of $\widetilde{O}(\Delta)$.

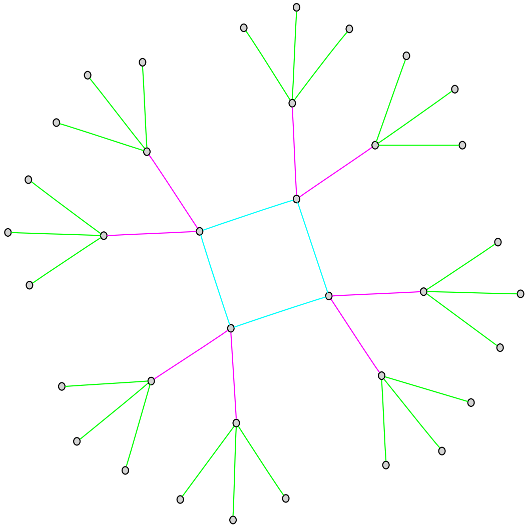
Vertical isogenies with elliptic curves

Remark

It is easier to find a curve in the isogeny class rather than in the subset of maximal curves. One can use vertical isogenies to go from such a curve to a maximal curve;

- ⇒ *This approach gain some logarithmic factors and yields huge practical improvements!*

Vertical isogenies with elliptic curves



Adapting these ideas to the genus 2 case

1. Select a CRT prime p;
2. Select random Jacobians until finding one in the right isogeny class;
3. Try to go up using vertical isogenies to find a Jacobian with CM by O_K;
4. Use horizontal isogenies to find all other Jacobians with CM by O_K;
5. From the invariants of the maximal abelian surfaces, reconstruct $H_{\Phi,i} \mod p$.

Obtaining all the maximal Jacobians: the horizontal isogenies

- 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 elements 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 Jacobians we will obtain with (ℓ,ℓ)-isogenies ($\Rightarrow$ Don't compute unneeded isogenies).
- Moreover, if J is a maximal Jacobian, and ℓ does not divide $(O_K : \mathbb{Z}[\pi,\overline{\pi}])$, then any (ℓ,ℓ)-isogenous Jacobian is maximal.

Remark

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.

Checking if a curve is maximal and going up

Cumbersome method: if A is in the isogeny class, compute $\mathrm{End}(A)$. If this is not O_K try to compute a vertical isogeny $f: A \to B$ with $\mathrm{End}(B) \supset \mathrm{End}(A)$. Recurse...

Intelligent method: try to go up at the same time we compute $\mathrm{End}(A)$.

Checking if a curve is maximal and going up

Cumbersome method: if A is in the isogeny class, compute $\mathrm{End}(A)$. If this is not O_K try to compute a vertical isogeny $f : A \to B$ with $\mathrm{End}(B) \supset \mathrm{End}(A)$. Recurse...

Intelligent method: try to go up at the same time we compute $\mathrm{End}(A)$.

The vertical method of Freeman-Lauter:

- Let $P(\pi)$ be a polynomial on the Frobenius. It is easy to compute its action on $A(\mathbb{F}_p)[n]$ provided we have a basis of the n-torsion. If this action is null, then $\gamma = P(\pi)/n \in K$ is actually an element of $\mathrm{End}(A)$

⇒ If $L = P(\pi)\left(A(\mathbb{F}_p)[n]\right) \neq \{0\}$, then L can be seen as the obstruction to $\gamma \in \mathrm{End}(A)$. We try to find isogenies such that this obstruction decrease, and recurse.

Checking if a curve is maximal and going up

Cumbersome method: if A is in the isogeny class, compute $\mathrm{End}(A)$. If this is not O_K try to compute a vertical isogeny $f : A \to B$ with $\mathrm{End}(B) \supset \mathrm{End}(A)$. Recurse...

Intelligent method: try to go up at the same time we compute $\mathrm{End}(A)$.

The horizontal method of Bisson-Sutherland:

- If $I_1^{n_1} I_2^{n_2} \dots I_k^{n_k}$ is a relation in $\mathfrak{C}(O_K)$, then if $\mathrm{End}(A) = O_K$, following the isogeny path corresponding to I_1 (n_1 times) followed by I_2 (n_2 times)...will give a cycle in the isogeny graph;

⇒ If instead at the end of the path we find an abelian variety B non isomorphic to A then we try to collapse the path by finding two isogenies of the same degree $f : A \to A'$ and $g : B \to A'$ to the same abelian variety. Starting from A' will then give us a cycle. Recurse from here...

Checking if a curve is maximal and going up

Cumbersome method: if A is in the isogeny class, compute $\mathrm{End}(A)$. If this is not O_K try to compute a vertical isogeny $f : A \to B$ with $\mathrm{End}(B) \supset \mathrm{End}(A)$. Recurse...

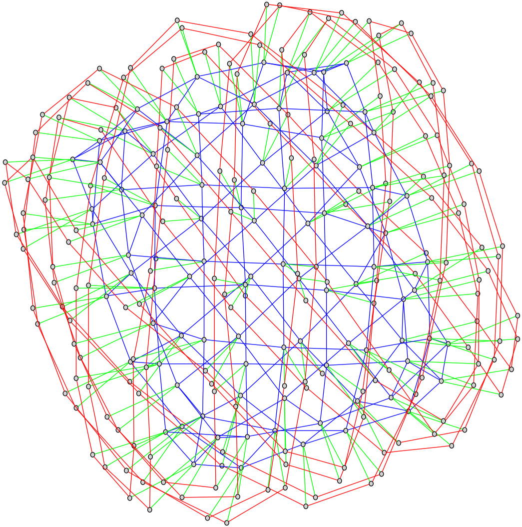
Intelligent method: try to go up at the same time we compute $\mathrm{End}(A)$.

Remark

Asymptotically the horizontal method is sub-exponential while the vertical method is exponential. In practice the horizontal method give huge speed up even in small examples when the index $[O_K : \mathbb{Z}[\pi, \overline{\pi}]]$ *is divisible by a power.*

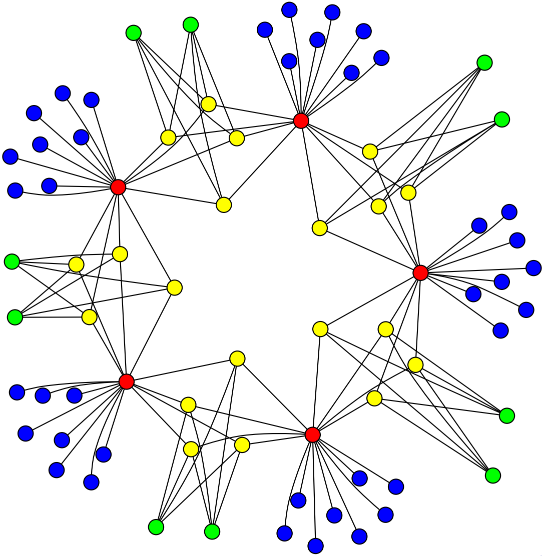
Some pesky details

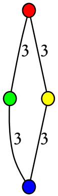
Non maximal cycles ⇒ We try to reduce globally the obstruction for all endomorphisms.



Some pesky details

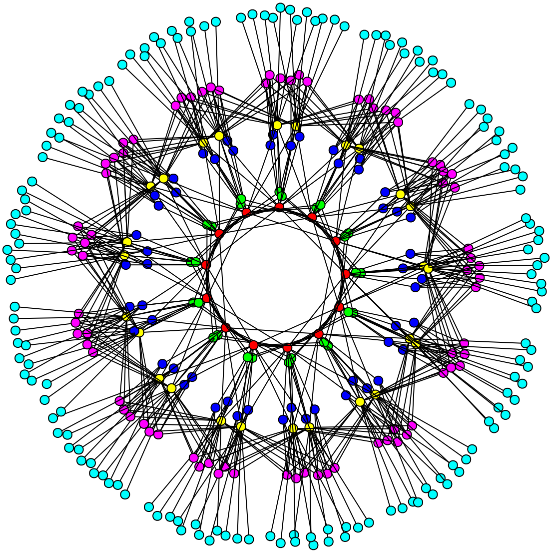
Local minimums I

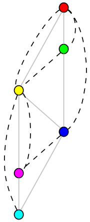




Some pesky details

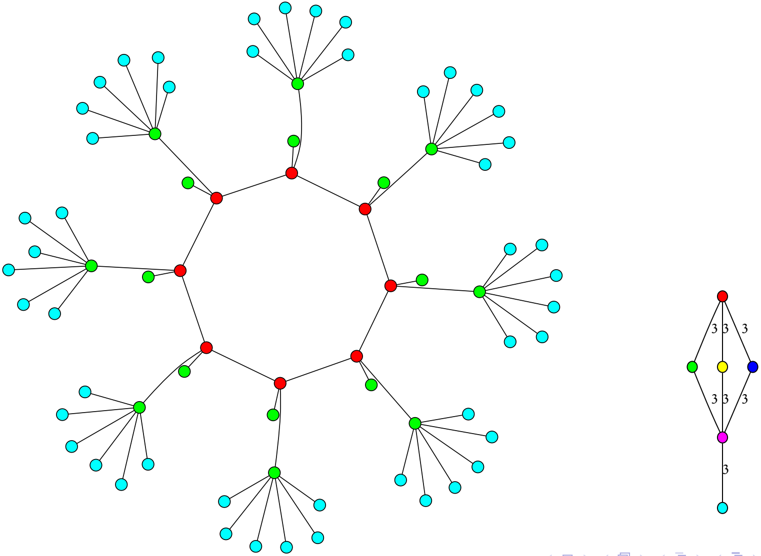
Local minimums II





Some pesky details

Polarizations



Some pesky details

- With the CRT primes p we are working with, there is $O(p^3)$ hyperelliptic curves (up to isomorphisms), $O(p^{3/2})$ curves in the isogeny class (corresponding to K) and only $O(p^{1/2})$ curves with maximal endomorphism ring O_K
  $\Rightarrow$ being able to go up gains more than logarithmic factors!
- Unfortunately 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).

Further details

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

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

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

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

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

p	l^d	α_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	α_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	3^3	18	81	54	$376+8.1$	$0.3+0.9$
107	$3^2,43$	$6,308$	-	-	-	-
113	$3,53$	$1,52$	159	155	$1118+137.2$	$0.8+25$
131	$3^2,53$	$6,52$	477	477	$1872+127.4$	$2.2+44.4$
139	3^5	81	?	486	-	$1+36.7$
157	3^4	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	α_d	# Curves	Estimate	Time (old)	Time (new)
7	-	-	1	1	0.3	$0+0.1$
23	$\mathbf{13}$	84	15	2 (16)	$9+70.7$	$0.4+24.6$
53	7	3	7	7	$105+0.5$	$7.7+0.5$
59	$2,\mathbf{5}$	$1,12$	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	$7,\mathbf{13}$	$3,21$	105	8 (107)	$963+69.3$	-
139	$\mathbf{5}^2,7$	$60,2$	259	9 (260)	$2189+62.1$	-
181	3	1	161	135	$5040+3.6$	$4.5+0.2$
197	$5,109$	$24,5940$	-	-	-	-
199	$\mathbf{5}^2$	60	37	2 (39)	$10440+35.1$	-
223	$2,\mathit{23}$	$1,11$	1058	39 (914)	$10440+35.1$	-
227	109	1485	-	-	-	-
233	$5,7,\mathbf{13}$	$8,3,28$	735	55 (770)	$11580+141.6$	$88.3+29.4$
239	$7,109$	$6,297$	-	-	-	-
257	$3,7,\mathbf{13}$	$4,6,84$	1155	109 (1521)	$17160+382.8$	-
313	$3,\mathbf{13}$	$1,14$	?	146 (2035)	-	$165+14.7$
373	$5,7$	$6,24$	?	312	-	$183.4+3.8$
541	$2,7,\mathbf{13}$	$1,3,14$	?	294 (4106)	-	$91+5.5$
571	$3,\mathbf{5},7$	$2,6,6$	?	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 α 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 $\widetilde{O}(\Delta_0^{1/2}\Delta_1^{1/2})$.
- 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 even if the going-up step always succeed!

$\Rightarrow$ 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;
- Use Ionica 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 (ℓ,ℓ)-isogenies.