Reducing number field defining polynomials: An application to class group computations

Alexandre Gélin and Antoine Joux

Laboratoire d'Informatique de Paris 6 – Sorbonne Universités UPMC

Chaire de Cryptologie, Fondation UPMC

ANTS XII – Kaiserslautern

2016/09/02

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} = \mathbf{Q}[X]/(T).$$

T is a defining polynomial of $\mathbf{K}$.

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} = \mathbf{Q}[X]/(T).$$

T is a defining polynomial of $\mathbf{K}$.

Two interesting structures:

- Group of ideals
- Group of units

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} = \mathbf{Q}[X]/(T).$$

T is a defining polynomial of $\mathbf{K}$.

Two interesting structures:

- Group of ideals

  Quotient by principal ideals $\Rightarrow$ class group $Cl(\mathscr{O}_{\mathbf{K}})$

- Group of units

  Finitely generated $\Rightarrow$ fundamental units

Number fields

$\mathbf{K}$ number field $\Rightarrow$ finite extension of $\mathbf{Q}$ $\Rightarrow$ $\exists T \in \mathbf{Z}[X]$ monic s.t.

$$\mathbf{K} = \mathbf{Q}[X]/(T).$$

T is a defining polynomial of $\mathbf{K}$.

Two interesting structures:

- Group of ideals

  Quotient by principal ideals $\Rightarrow$ class group $Cl(\mathscr{O}_{\mathbf{K}})$

- Group of units

  Finitely generated $\Rightarrow$ fundamental units

Aim: Compute the structure of the class group.

State of the art

Subexponential L-notation : $L_N(0,c) \approx (\log N)^c$ $L_N(1,c) \approx N^c$

$$L_N(\alpha, c) = \exp\left((c + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right).$$

- Based on index calculus method
- Work from Biasse and Fieker, 2014

General case

Under GRH and smoothness heuristics, they have an $L_{|\Delta_{\mathbf{K}}|}(\frac{2}{3} + \varepsilon)$ algorithm for class group and unit group computation and an $L_{|\Delta_{\mathbf{K}}|}(\frac{1}{2})$ one if $n \leq \log(|\Delta_{\mathbf{K}}|)^{3/4-\varepsilon}$.

Conditional case

If $\mathbf{K}$ is defined by a *good* polynomial, we may reach a runtime in $L_{|\Delta_{\mathbf{K}}|}(a)$, with $\frac{1}{3} \leq a < \frac{1}{2}$.

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

Definition

Let $T = \sum a_k X^k \in \mathbf{Z}[X]$. The height of T is defined as the maximal norm of its coefficients, namely

$$H(T) = \max_k |a_k|.$$

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

Definition

Let $T = \sum a_k X^k \in \mathbf{Z}[X]$. The height of T is defined as the maximal norm of its coefficients, namely

$$H(T) = \max_k |a_k|.$$

Proposition

For every defining polynomial T of a degree-n number field $\mathbf{K}$, the discriminants satisfy

$$|\Delta_{\mathbf{K}}| \leq |\Delta(T)| \leq n^{2n} H(T)^{2n-2}.$$

Classes from Biasse and Fieker work

Definition

Let $n_0, d_0 > 0$ and $0 < \alpha < \frac{1}{2}$.

$$\mathscr{C}_{n_0,d_0,\alpha} = \left\{ \mathbf{K} = \mathbf{Q}[X]/(T) \middle| \begin{array}{l} \deg(T) = n_0(\log|\Delta_{\mathbf{K}}|)^{\alpha}(1+o(1)) \\ \log H(T) = d_0(\log|\Delta_{\mathbf{K}}|)^{1-\alpha}(1+o(1)) \end{array} \right\}$$

Theorem

There exists an $L_{|\Delta_{\mathbf{K}}|}(a)$ algorithm for class group computation for

$$a = \max\left(\alpha, \frac{1-\alpha}{2}\right).$$

Minimal height

If $\mathbf{K} \in \mathscr{C}_{n_0,d_0,\alpha}$, there exists T such that

$$H(T) = |\Delta_{\mathbf{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Minimal height

If $\mathbf{K} \in \mathscr{C}_{n_0,d_0,\alpha}$, there exists T such that

$$H(T) = |\Delta_{\mathbf{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Proposition

For every number field $\mathbf{K}$, there exists a defining polynomial T s.t.

$$H(T) \leq 3^n \left(\frac{|\Delta_{\mathbf{K}}|}{n} \right)^{\frac{n}{2n-2}}.$$

Minimal height

If $\mathbf{K} \in \mathscr{C}_{n_0,d_0,\alpha}$, there exists T such that

$$H(T) = |\Delta_{\mathbf{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Proposition

For every number field $\mathbf{K}$, there exists a defining polynomial T s.t.

$$H(T) \leq 3^n \left(\frac{|\Delta_{\mathbf{K}}|}{n} \right)^{\frac{n}{2n-2}}.$$

Definition

Let $n_0, d_0 > 0$, $0 < \alpha < 1$ **and** $1 - \alpha \leq \gamma \leq 1$.

$$\mathscr{D}_{n_0,d_0,\alpha,\gamma} = \left\{ \mathbf{K} = \frac{\mathbf{Q}[X]}{(T)} \;\middle|\; \begin{array}{l} \deg(T) \leq n_0 \left(\frac{\log|\Delta_{\mathbf{K}}|}{\log\log|\Delta_{\mathbf{K}}|} \right)^{\alpha} \\ \log H(T) \leq d_0 (\log|\Delta_{\mathbf{K}}|)^{\gamma} (\log\log|\Delta_{\mathbf{K}}|)^{1-\gamma} \end{array} \right\}$$

Minimal height

If $\mathbf{K} \in \mathscr{C}_{n_0,d_0,\alpha}$, there exists T such that
$$H(T) = |\Delta_{\mathbf{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Proposition

For every number field $\mathbf{K}$, there exists a defining polynomial T s.t.
$$H(T) \leq 3^n \left(\frac{|\Delta_{\mathbf{K}}|}{n} \right)^{\frac{n}{2n-2}}.$$

Definition

Let $n_0, d_0 > 0$, $0 < \alpha < 1$ **and** $1 - \alpha \leq \gamma \leq 1$.

$$\mathscr{D}_{n_0,d_0,\alpha,\gamma} = \left\{ \mathbf{K} = \frac{\mathbf{Q}[X]}{(T)} \;\middle|\; \begin{array}{l} \deg(T) \leq n_0 \left(\frac{\log|\Delta_{\mathbf{K}}|}{\log\log|\Delta_{\mathbf{K}}|} \right)^{\alpha} \\ \log H(T) \leq d_0 (\log|\Delta_{\mathbf{K}}|)^{\gamma} (\log\log|\Delta_{\mathbf{K}}|)^{1-\gamma} \end{array} \right\}$$

Every number field belongs to such a class $\mathscr{D}_{n_0,d_0,\alpha,\gamma}$.

Prior reduction algorithm

Cohen and Diaz y Diaz minimize the size of $T = \prod(X - \tau_j)$, defined as

$$S(T) = \sum |\tau_j|^2.$$

Equivalent to find a short vector in the lattice $\mathscr{O}_{\mathbf{K}}$, because $\mathscr{O}_{\mathbf{K}}$ is generated by the vectors

$$\left[\sigma_1(\tau_j), \cdots, \sigma_n(\tau_j)\right]$$

☺ **Examples:**

Input	Output
$x^3 - 5955x^2 + 18142x - 607593$	$x^3 - x^2 - 2100x + 38117$
$x^3 - 269463x^2 + 752031x - 518157$	$x^3 - x^2 - 1307x - 13359$
$x^3 - 482665x^2 + 773338x - 308749$	$x^3 - x^2 - 3210x + 61325$
$x^3 - 456191x^2 + 958783x - 499681$	$x^3 - x^2 - 936x - 7616$

Prior reduction algorithm

Cohen and Diaz y Diaz minimize the size of $T = \prod(X - \tau_j)$, defined as

$$S(T) = \sum |\tau_j|^2.$$

Equivalent to find a short vector in the lattice $\mathcal{O}_\mathbf{K}$, because $\mathcal{O}_\mathbf{K}$ is generated by the vectors

$$\left[\sigma_1(\tau_j), \cdots, \sigma_n(\tau_j)\right]$$

☹ **Examples:**

Input	Output
$x^3+6381x^2+4378x-1216$	$x^3-x^2-3537064x+2193757452$
$x^3-9681x^2-5434x-6901$	$x^3-31246021x-67226458585$
$x^3-6665x^2-4318x-2977$	$x^3+336681x-419200237$
$x^3-6018x^2-1387x+6161$	$x^3-12073495x-16147208593$

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbf{K}$.

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbf{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbf{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Let θ_F root of $T_F \longleftrightarrow v(\theta_F) = [\sigma_1(\theta_F), \cdots, \sigma_n(\theta_F)] \in \mathscr{O}_{\mathbf{K}}$.

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbf{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Let θ_F root of $T_F \longleftrightarrow v(\theta_F) = [\sigma_1(\theta_F), \cdots, \sigma_n(\theta_F)] \in \mathscr{O}_{\mathbf{K}}$.

Let $c > 1$ and $b^F = [b_1^F, \cdots, b_n^F]$ defined by $b_j^F = \left\lceil \log_c |\sigma_j(\theta_F)| \right\rceil$.
We introduce a *weighted* copy of $\mathscr{O}_{\mathbf{K}}$ in $\mathscr{C}^n$, generated by:

$$\widetilde{\Omega_i} = \left[\frac{\sigma_1(\omega_i)}{c^{b_1^F}}, \cdots, \frac{\sigma_n(\omega_i)}{c^{b_n^F}} \right].$$

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbf{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Let θ_F root of $T_F \longleftrightarrow v(\theta_F) = [\sigma_1(\theta_F), \cdots, \sigma_n(\theta_F)] \in \mathcal{O}_{\mathbf{K}}$.

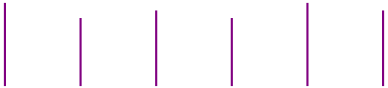
Let $c > 1$ and $b^F = [b_1^F, \cdots, b_n^F]$ defined by $b_j^F = \lceil \log_c |\sigma_j(\theta_F)| \rceil$.
We introduce a *weighted* copy of $\mathcal{O}_{\mathbf{K}}$ in $\mathscr{C}^n$, generated by:

$$\widetilde{\Omega_i} = \left[\frac{\sigma_1(\omega_i)}{c^{b_1^F}}, \cdots, \frac{\sigma_n(\omega_i)}{c^{b_n^F}} \right].$$

By construction, $|\tilde{v}(\theta_F)_i| \leq 1$ and $\|\tilde{v}(\theta_F)\|_2 \leq \sqrt{n}$.

Differences between the two algorithms

Shape of the vectors found by the algorithm of Cohen:



Shape of the vectors we find:

As the constant coefficient of the polynomial is the product of all the roots, we prefer vectors of the second family.

Final results

- If $\mathbf{K} \in \mathscr{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal defining polynomial T in time $L_{|\Delta_{\mathbf{K}}|}(\alpha)$.

Final results

- If $\mathbf{K} \in \mathscr{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal defining polynomial T in time $L_{|\Delta_\mathbf{K}|}(\alpha)$.

- If $\gamma = 1 - \alpha$, we can apply the algorithm of Biasse and Fieker and find the class group in $L_{|\Delta_\mathbf{K}|}(a)$, $a = \max\left(\alpha, \frac{1-\alpha}{2}\right)$.

Final results

- If $\mathbf{K} \in \mathscr{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal defining polynomial T in time $L_{|\Delta_{\mathbf{K}}|}(\alpha)$.

- If $\gamma = 1-\alpha$, we can apply the algorithm of Biasse and Fieker and find the class group in $L_{|\Delta_{\mathbf{K}}|}(a)$, $a = \max\left(\alpha, \frac{1-\alpha}{2}\right)$.

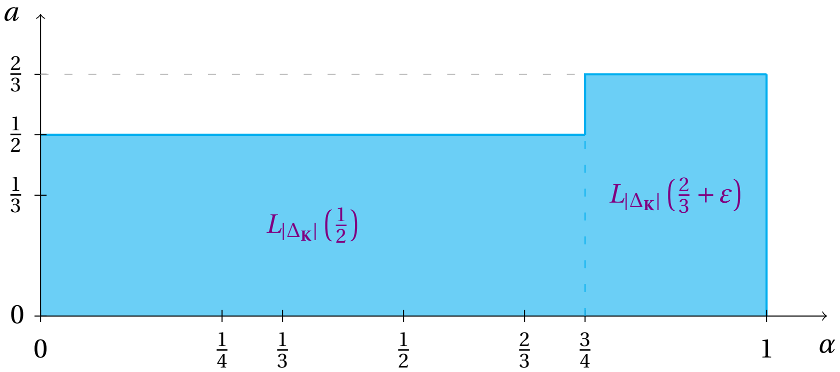
Theorem

Under GRH and smoothness heuristics, for every $\mathbf{K} \in \mathscr{D}_{n_0,d_0,\alpha,\gamma}$, $\alpha < \frac{1}{2}$, there exists an $L_{|\Delta_{\mathbf{K}}|}(a)$ algorithm for class group computation with

$$a = \max\left(\alpha, \frac{\gamma}{2}\right).$$

State of the art [BF14]

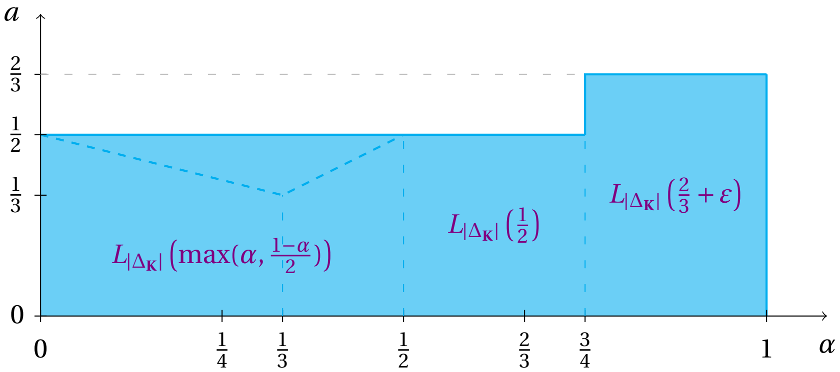
General case:



First general subexponential algorithm.

State of the art [BF14]

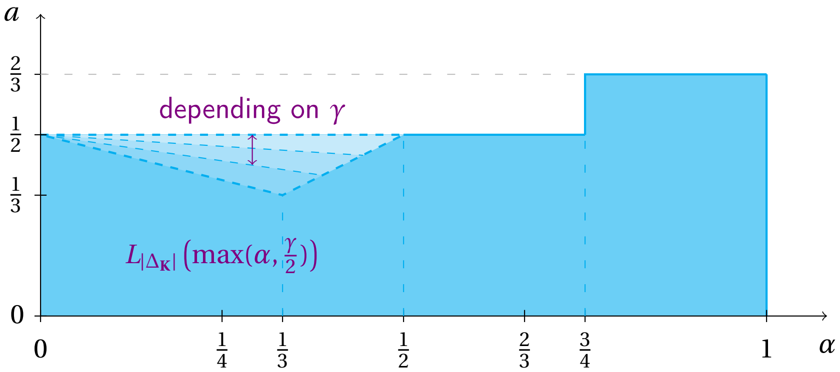
Special case:



Only if $\mathbf{K}$ is defined by T such that $H(T) = L_{|\Delta_{\mathbf{K}}|}(1-\alpha)$.

This work

General case:



Without any condition.

Practically

$\mathbf{K}$ is defined by the polynomial

$$x^5 - 2x^4 - 8001397580x^3 - 31542753393650x^2 + 3636653302451131875x + 4818547529425280067500$$

Magma V2.22-2 finds the class group – assuming GRH – in about 285 seconds.

With our implementation, we reduce this defining polynomial to

$$T = x^5 - 5843635x^4 + 931633x^2 + 6577x - 8570.$$

Practically

$\mathbf{K}$ is defined by the polynomial

$$x^5 - 2x^4 - 8001397580x^3 - 31542753393650x^2 + 3636653302451131875x + 4818547529425280067500$$

Magma V2.22-2 finds the class group – assuming GRH – in about 285 seconds.
With our implementation, we reduce this defining polynomial to

$$T = x^5 - 5843635x^4 + 931633x^2 + 6577x - 8570.$$

Magma V2.19-10 has class group computation not as optimized as in V2.22, but works with the input polynomial:

- with T: about 140 seconds,
- with the "reduced" one: about 3240 seconds.

Thanks

Danke