**Isogeny-based Cryptography School** **Summer 2021**

# Lecture 8: Class groups of large degree fields

*Lecturer: Jean-François Biasse* *TA: R. Erukulangara and W. Youmans*



In this lecture, we recall the main result of the subexponential method for computing the class group and solving the PIP in number fields of large degree of [1, 2].

## 8.1 BKZ reduction of ideals

The main ingredient of the computation of class groups in large degree number fields is a reduction algorithm that takes as input an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ and returns another ideal of norm bounded by the invariant of the fields only in the same ideal class as $\mathfrak{a}$.

**Algorithm 1** BKZ-ideal reduction

**Require:** $\mathfrak{a} \in \mathcal{O}_K$, and block size $k > 0$.
**Ensure:** $\alpha \in K$ such that $(\alpha) \cdot \mathfrak{a} \subseteq \mathcal{O}_K$ has bounded norm.
1: $\frac{\mathfrak{c}}{l} \leftarrow \mathfrak{a}^{-1}$ where $\mathfrak{c} \subseteq \mathcal{O}_K$, and $l > 0$.
2: $\gamma \leftarrow$ first element of a BKZ-reduced basis of $\mathfrak{c}$ with block size $k$.
3: **return** $\frac{\gamma}{l}$

**Proposition 8.1** *Algorithm 1 with $k = n^{2/3}$ runs in time*

$$\mathrm{Poly}(\log|\Delta_K|, \log(\mathrm{N}(\mathfrak{a}))) \cdot 2^{\tilde{O}(n^{2/3})},$$

*and returns $\alpha = \gamma/l$ such that*

- $\mathrm{N}((\alpha) \cdot \mathfrak{a}) \leq 2^{\tilde{O}(n^{4/3})}\sqrt{|\Delta_K|}$.
- $\log(l), \log\|\gamma\| \in \mathrm{Poly}(\log(\mathrm{N}(\mathfrak{a})), \log|\Delta_K|)$.

**Proof:** BKZ with block size $k$ returns $\gamma \in \mathfrak{c}$ such that

$$\|\gamma\| \leq k^{n/2k}|\Delta_K|^{1/2n}\mathrm{N}(\mathfrak{c})^{1/n}$$

in time $2^{\tilde{O}(k)} \cdot \mathrm{Poly}(\log|\Delta_K|, \log(\mathrm{N}(\mathfrak{c})))$. Moreover, we have $\mathrm{N}(\mathfrak{a}) \leq l$ and

$$\mathrm{N}(\mathfrak{c}) \leq l^n/\mathrm{N}(\mathfrak{a}) \leq l^{n-1} \leq \mathrm{N}(\mathfrak{a})^{n-1} \leq \mathrm{N}(I)^n.$$

This proves the bounds on the size of $l$ and $\|\gamma\|$. Additionally, we have

$$\mathrm{N}((\alpha) \cdot \mathfrak{a}) = \frac{\mathrm{N}(\gamma)}{\mathrm{N}(l)}\mathrm{N}(\mathfrak{a}) = \frac{\mathrm{N}(\gamma)}{\mathrm{N}(l)}\frac{\mathrm{N}(l)}{\mathrm{N}(\mathfrak{c})} \leq \frac{\|\gamma\|^n}{\mathrm{N}(\mathfrak{c})} \leq \frac{2^{\tilde{O}(n^{4/3})}\sqrt{|\Delta_K|}\mathrm{N}(\mathfrak{c})}{\mathrm{N}(\mathfrak{c})},$$

which shows the bound on the norm of the reduced ideal $(\alpha)\mathfrak{a}$. ■

## 8.2 Relations between ideals

Given an input ideal $\mathfrak{a}$ and factor basis of prime ideals $\mathcal{B}$ whose classes generate $\mathrm{Cl}(\mathcal{O}_K)$, we want to return a decomposition of the ideal class of $\mathfrak{a}$ over $\langle\mathcal{B}\rangle$. This is done by multiplying short products of primes in $\mathcal{B}$, BKZ-reducing the resulting ideal, and checking whether it decomposes as a product of elements in $\mathcal{B}$. We assume that $S = \{\mathfrak{p} \text{ prime ideals with } \mathrm{N}(\mathfrak{p}) \leq 2^{(\log|\Delta_K|)^{2/3}}\}$. As in the quadratic case, we use the fact that under the GRH, primes of norm up to $12(\log|\Delta_K|)^2$ generate $\mathrm{Cl}(\mathcal{O}_K)$, and that the class of an ideal multiplied by a short product of such primes is almost uniformly distributed in $\mathrm{Cl}(\mathcal{O}_K)$. This procedure is described in Algorithm 2. As of now, the run time of Algorithm 2 is only heuristic. The probability of $(\alpha)\cdot\mathfrak{a}'$

**Algorithm 2** Decomposition of an ideal

**Require:** $\mathfrak{a} \in \mathcal{O}_K$.

**Ensure:** $\alpha \in K$, and $(x_i)_{i\leq l} \in \mathbb{Z}^l$ with $(\alpha)\cdot\mathfrak{a} = \prod_i \mathfrak{p}_i^{x_i}$ and $\mathrm{N}(\mathfrak{p}_i) \leq 2^{\tilde{O}((\log|\Delta_K|)^{2/3})}$.

1: $S = \{\mathfrak{p} \text{ prime ideals with } \mathrm{N}(\mathfrak{p}) \leq 2^{(\log|\Delta_K|)^{2/3}}\}$, and $l \leftarrow |\mathcal{B}|$.<br>
2: $S_0 = \{\mathfrak{p} \text{ prime ideals with } \mathrm{N}(\mathfrak{p}) \leq 12(\log|\Delta_K|)^2\}$, and $l_0 \leftarrow |\mathcal{B}|$<br>
3: **while** true **do**<br>
4:     $(x_i) \xleftarrow{\mathcal{R}} [0, \log|\Delta_K|]^{l_0}$. $\mathfrak{a}' \leftarrow \mathfrak{a}\cdot\prod_{i\leq l_0}\mathfrak{p}_i^{x_i}$.<br>
5:     Compute $\alpha$ with Algorithm 1 on input $\mathfrak{a}'$, $k = n^{2/3}$.<br>
6:     **if** $(\alpha)\cdot\mathfrak{a}'$ is $\mathcal{B}$-smooth **then**<br>
7:         Compute $\vec{y}$ such that $(\alpha)\cdot\mathfrak{a}' = \prod_{i\leq l}\mathfrak{p}_i^{y_i}$.<br>
8:         $\vec{x} \leftarrow \vec{y} - \vec{x}||\vec{0}$.<br>
9:         **return** $\alpha, \vec{x}$<br>
10:     **end if**<br>
11: **end while**

being $\mathcal{B}$-smooth is not rigorously understood at this point, but there are rigorous results mentioned in [2, Sec. 3.1] showing that the proportion of ideals of norm less than $\iota$ that are a product of prime ideals of norm less than $\mu$ is $e^{-u\log(u)(1+o(1))}$ where $u = \log(\iota)/\log(\mu)$. Heuristic 1 of [2, Sec. 3.1] conjectures that this is also the smoothness probability of the reduced ideal $(\alpha)\cdot\mathfrak{a}'$ of Step 6. Due to the fact that the Cayley graph of $\mathrm{Cl}(\mathcal{O}_K)$ is an expander, we can argue that the ideal class of $\mathfrak{a}'$ is distributed almost uniformly at random, but so far, there is no rigorous proof of how the multiplication by $\alpha$ obtained with Algorithm 1 influences the smoothness probability.

**Conjecture 1 (Heuristic 1 of [2])** *Let $k > 0$, and let $\mathfrak{a}$ be an ideal in a class of $\mathrm{Cl}(\mathcal{O}_K)$ that is drawn uniformly at random, and let $\mathfrak{a}'$ be the output of Algorithm 1 with input $\mathfrak{a}, k$. Then the probability of $I'$ being a product of prime ideals of norm less than $\mu$ is $e^{-u\log(u)(1+o(1))}$ where $u = \log(\mathrm{N}(\mathfrak{a}'))/\log(\mu)$.*

**Proposition 8.2 (under GRH and Conjecture 1)** *Algorithm 2 is correct and has asymptotic complexity in $\mathrm{Poly}(\log(\mathrm{N}(I)))\cdot 2^{\tilde{O}\left((\log|\Delta_K|)^{2/3}\right)}$ and returns $\alpha = \gamma/l \in K$, $\vec{x} \in \mathbb{Z}^l$ such that $(\alpha)\cdot I = \prod_{i\leq l}\mathfrak{p}_i^{x_i}$ with $\gamma, l, \vec{x}$ of polynomial size.*

**Proof:** We apply Proposition 8.1 to the ideal $\mathfrak{a}' = \mathfrak{a}\cdot\prod_{i\leq l_0}\mathfrak{p}_i^{x_i}$. It satisfies $\log(\mathrm{N}(\mathfrak{a}')) \in \mathrm{Poly}(\log(\mathrm{N}(\mathfrak{a})), \log|\Delta_K|)$, which proves the bound on the size of $\|\gamma\|$ and $l$. Moreover, the runtime is $\mathrm{Poly}(\log(\mathrm{N}(\mathfrak{a})))\cdot 2^{\tilde{O}(k)}$ where $k$ is the block size used for the BKZ reduction, hence giving us the cost of one reduction. Then, assuming Conjecture 1, the probability that the resulting reduced ideals $\mathfrak{a}'$ whose norms satisfy $\log(\mathrm{N}(\mathfrak{a}')) \in \tilde{O}\left((\log|\Delta_K|)^{4/3}\right)$ be $S$-smooth is in

$$\frac{1}{2^{\tilde{O}\left(\frac{(\log|\Delta_K|)^{4/3}}{(\log|\Delta_K|)^{2/3}}\right)}} = \frac{1}{2^{\tilde{O}\left((\log|\Delta_K|)^{2/3}\right)}}.$$

This shows that the expected cost to find a relation is in Poly $(\log(\mathrm{N}(\mathfrak{a}))) \cdot 2^{\tilde{O}\left((\log|\Delta_K|)^{2/3}\right)}$. Finally, the size of the output vector derives from the fact that it is of the form $\vec{y} - \vec{x}||\vec{0}$ where $\log\|\vec{x}\| \in \mathrm{Poly}(\log|\Delta_K|)$ by construction, while $\vec{y}$ is the decomposition of the BKZ-reduced ideal $\mathfrak{a}'$ with respect to $\mathcal{B}$.

■

## 8.3 Computation of the class group

The general strategy to compute the class group is to apply Algorithm 2 to $I = \mathcal{O}_K$ as many times as it takes in order to compute a basis for the lattice $\Lambda$ of vectors $\vec{x} \in \mathbb{Z}^l$ such that $\prod_i \mathfrak{p}_i^{x_i} \sim (1)$, i.e. the so-called *lattice of relations* between elements of $\mathcal{B}$. To justify the run time of this class group procedure, we need to make an additional heuristic, which corresponds to Heuristic 3 of [2]. It argues that the relations drawn during Algorithm 2 are well-enough distributed among the full lattice of relations between classes of primes in $\mathcal{B}$. Even though Algorithm 2 uses randomization, we have no guarantee on the distribution of the relations we create. In [3, Sec. 3.1], Hafner and McCurley show how to estimate this distribution rigorously in the case of quadratic fields, and they show in [3, Sec. 3.2] that once a sublattice of rank $|\mathcal{B}|$ is found, only $|\mathcal{B}|^{1+o(1)}$ extra relations need to be found randomly to complete the lattice of relations.

**Conjecture 2 (Heuristic 3 of [2])** *With probability* $1 - 1/|\Delta_K|$*, the number of iterations of the relation search procedure given by Algorithm 2 is bounded by* $|\mathcal{B}|^{1+o(1)}$.

## References

[1] J.-F. Biasse. Subexponential time relations in the class group of large degree number fields. *Advances in Mathematics of Communications*, 8(4):407–425, 2014.

[2] J.-F. Biasse and C. Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS J. Comput. Math.*, 17(suppl. A):385–403, 2014.

[3] J.L. Hafner and K.S. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of American Society*, 2:839–850, 1989.