Sampling relatively factorizable elements in ideals of number fields

Alice Pellet-Mary

CNRS, université de Bordeaux

Séminaire Caramba, Nancy

Joint work with Koen de Boer, Léo Ducas and Benjamin Wesolowski

Outline of the talk

Outline of the talk

1. Definitions and problem statement
2. Our result
3. Application: computing units

Number fields

- K number field
- R its ring of integers
- n its degree
  - $n = 512$
  - $K = \mathbb{Q}[X]/(X^n + 1)$
  - $R = \mathbb{Z}[X]/(X^n + 1)$

Number fields

- K number field
- R its ring of integers
- n its degree
  - $n = 512$
  - $K = \mathbb{Q}[X]/(X^n + 1)$
  - $R = \mathbb{Z}[X]/(X^n + 1)$
- n measures the "bit-size" of K
  (assume $\log |\Delta_K| \approx n$ for the talk)
  - efficient algorithm $\Leftrightarrow$ poly(n)

Ideals and units

- Units: $R^\times = \{a \in R \mid \exists b \in R, ab = 1\}$
  - e.g. $\mathbb{Z}^\times = \{-1, 1\}$

Ideals and units

- Units: $R^\times = \{a \in R \mid \exists b \in R, ab = 1\}$
  - e.g. $\mathbb{Z}^\times = \{-1, 1\}$
- Principal ideals: $\langle g \rangle := \{gr \mid r \in R\}$ (i.e. all multiples of g)
  - e.g. $\langle 2 \rangle = \{\text{even numbers}\}$; $\langle 1/2 \rangle = \{r/2, r \in \mathbb{Z}\}$
  - g is called a generator of $\langle g \rangle$
  - The generators of $\langle g \rangle$ are exactly the ug for $u \in R^\times$

Ideals and units

- Units: $R^\times = \{a \in R \mid \exists b \in R, ab = 1\}$
  - e.g. $\mathbb{Z}^\times = \{-1, 1\}$

- Principal ideals: $\langle g \rangle := \{gr \mid r \in R\}$ (i.e. all multiples of g)
  - e.g. $\langle 2 \rangle = \{\text{even numbers}\}$; $\langle 1/2 \rangle = \{r/2, r \in \mathbb{Z}\}$
  - g is called a generator of $\langle g \rangle$
  - The generators of $\langle g \rangle$ are exactly the ug for $u \in R^\times$

Representation

An ideal $I = \langle g \rangle$ is represented by a basis $x_1, \cdots, x_n \in I$ such that

$$I = \{\sum_i n_i \cdot x_i \, , \, n_i \in \mathbb{Z}\}.$$

(I is **not** represented by g)

Properties of ideals

Properties:

- $I \cdot J$ $(\langle g \rangle \cdot \langle h \rangle = \langle gh \rangle)$, I^{-1} $(\langle g \rangle^{-1} = \langle g^{-1} \rangle)$, $\langle 1 \rangle = R$

Properties of ideals

Properties:

- $I \cdot J$ $(\langle g \rangle \cdot \langle h \rangle = \langle gh \rangle)$, I^{-1} $(\langle g \rangle^{-1} = \langle g^{-1} \rangle)$, $\langle 1 \rangle = R$
- notion of prime ideals $\mathfrak{p} \subseteq R$
- unique factorization: $I = \prod_i \mathfrak{p}_i^{\alpha_i}$, $\alpha_i \in \mathbb{Z}$

Properties of ideals

Properties:

- $I \cdot J$ $(\langle g\rangle \cdot \langle h\rangle = \langle gh\rangle)$, I^{-1} $(\langle g\rangle^{-1} = \langle g^{-1}\rangle)$, $\langle 1\rangle = R$
- notion of prime ideals $\mathfrak{p} \subseteq R$
- unique factorization: $I = \prod_i \mathfrak{p}_i^{\alpha_i}$, $\alpha_i \in \mathbb{Z}$

Algebraic norm:

- $\mathcal{N}(I) \in \mathbb{R}_+$ measures the "size" of I ($\approx$ absolute value)
- $\mathcal{N}(IJ) = \mathcal{N}(I) \cdot \mathcal{N}(J)$, $\mathcal{N}(I^{-1}) = \mathcal{N}(I)^{-1}$, $\mathcal{N}(R) = 1$
- if $I \subset R$, then $\mathcal{N}(I) \in \mathbb{Z}$.

Properties of ideals

Properties:

- $I \cdot J$ $(\langle g \rangle \cdot \langle h \rangle = \langle gh \rangle)$, I^{-1} $(\langle g \rangle^{-1} = \langle g^{-1} \rangle)$, $\langle 1 \rangle = R$
- notion of prime ideals $\mathfrak{p} \subseteq R$
- unique factorization: $I = \prod_i \mathfrak{p}_i^{\alpha_i}$, $\alpha_i \in \mathbb{Z}$

Algebraic norm:

- $\mathcal{N}(I) \in \mathbb{R}_+$ measures the "size" of I ($\approx$ absolute value)
- $\mathcal{N}(IJ) = \mathcal{N}(I) \cdot \mathcal{N}(J)$, $\mathcal{N}(I^{-1}) = \mathcal{N}(I)^{-1}$, $\mathcal{N}(R) = 1$
- if $I \subset R$, then $\mathcal{N}(I) \in \mathbb{Z}$.

Computational problems:

- $I \cdot J$, I^{-1}, $\gcd(I, J)$, $\mathcal{N}(I) \Rightarrow \mathrm{poly}(n)$
- recovering a generator g of $I \Rightarrow \mathrm{poly}(n)$ quantum or $L_{2/3}(n)$ classical
- computing the units $R^\times \Rightarrow \mathrm{poly}(n)$ quantum or $L_{2/3}(n)$ classical

Problem statement

Let $\mathcal{S} \subseteq \{I \text{ ideal}\}$. E.g.,

- B-smooth ideals: $\mathcal{S} = \{I = \prod_i \mathfrak{p}_i^{\alpha_i} \,|\, \mathcal{N}(\mathfrak{p}_i) \leq B\}$
- near-prime ideals: $\mathcal{S} = \{I = \mathfrak{p}_0 \cdot \prod_{i \geq 1} \mathfrak{p}_i^{\alpha_i} \,|\, \mathfrak{p}_0 \text{ prime}, \mathcal{N}(\mathfrak{p}_i) \leq B\}$
- co-prime with I_0: $\mathcal{S} = \{I \,|\, \gcd(I, I_0) = \langle 1 \rangle\}$

Problem statement

Let $\mathcal{S} \subseteq \{I \text{ ideal}\}$. E.g.,

- B-smooth ideals: $\mathcal{S} = \{I = \prod_i \mathfrak{p}_i^{\alpha_i} \,|\, \mathcal{N}(\mathfrak{p}_i) \leq B\}$
- near-prime ideals: $\mathcal{S} = \{I = \mathfrak{p}_0 \cdot \prod_{i \geq 1} \mathfrak{p}_i^{\alpha_i} \,|\, \mathfrak{p}_0 \text{ prime}, \mathcal{N}(\mathfrak{p}_i) \leq B\}$
- co-prime with I_0: $\mathcal{S} = \{I \,|\, \gcd(I, I_0) = \langle 1 \rangle\}$

Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Problem statement

Let $\mathcal{S} \subseteq \{I \text{ ideal}\}$. E.g.,

- B-smooth ideals: $\mathcal{S} = \{I = \prod_i \mathfrak{p}_i^{\alpha_i} \,|\, \mathcal{N}(\mathfrak{p}_i) \leq B\}$
  - [BF14], heuristic
- near-prime ideals: $\mathcal{S} = \{I = \mathfrak{p}_0 \cdot \prod_{i\geq 1} \mathfrak{p}_i^{\alpha_i} \,|\, \mathfrak{p}_0 \text{ prime}, \mathcal{N}(\mathfrak{p}_i) \leq B\}$
  - [BP17], heuristic
- co-prime with I_0: $\mathcal{S} = \{I \,|\, \gcd(I, I_0) = \langle 1 \rangle\}$
  - [RSW18], proven

Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

[BF14] Biasse and Fieker. Subexponential class group and unit group computation in large degree number Fields. LMS Journal of Computation and Mathematics.

[BP17] de Boer and Pagano. Calculating the power residue symbol and ibeta. ISSAC.

[RSW18] Rosca, Stehlé and Wallet. On the Ring-LWE and Polynomial-LWE problems. Eurocrypt.

Our result

Recall: Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Our result

Recall: Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Theorem

For some sets $\mathcal{S}$, we can solve Problem ★ provably (i.e., without heuristics) in $\mathrm{poly}(n)$ time.

Our result

Recall: Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Theorem

For some sets $\mathcal{S}$, we can solve Problem ★ provably (i.e., without heuristics) in $\mathrm{poly}(n)$ time.

$\mathcal{S}$ should satisfy

- a random ideal I is in $\mathcal{S}$ with non-negligible probability
- for some $B = \mathrm{poly}(n)$, if $I \in \mathcal{S}$, then $I \cdot J \in \mathcal{S}$ for any J that is B-smooth

Outline of the talk

General idea

Recall: Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Wlog, assume $\mathcal{N}(I) = 1$

General idea

Recall: Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Wlog, assume $\mathcal{N}(I) = 1$

Algorithm:

- Sample $x \leftarrow I$ randomly
- Repeat until $x \cdot I^{-1} \in \mathcal{S}$

General idea

Recall: Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Wlog, assume $\mathcal{N}(I) = 1$

Algorithm:

- Sample $x \leftarrow I$ randomly
- Repeat until $x \cdot I^{-1} \in \mathcal{S}$

Heuristic:

$$\Pr_{x \leftarrow I}(x \cdot I^{-1} \in \mathcal{S}) \approx \delta_S[\beta^n],$$

$\delta_S[\beta^n] = \frac{|\mathcal{S} \cap \{I \,|\, \mathcal{N}(I) \leq \beta^n\}|}{|\{I \,|\, \mathcal{N}(I) \leq \beta^n\}|}$ is the density of $\mathcal{S}$ (among ideals of norm $\leq \beta^n$)

General idea

Recall: Problem ★

Given an ideal $I = \langle g \rangle$, find $x = gr \in I$ such that $\langle x \rangle \cdot I^{-1} = \langle r \rangle \in \mathcal{S}$.

Wlog, assume $\mathcal{N}(I) = 1$

Algorithm:

- Sample $x \leftarrow I$ randomly
- Repeat until $x \cdot I^{-1} \in \mathcal{S}$

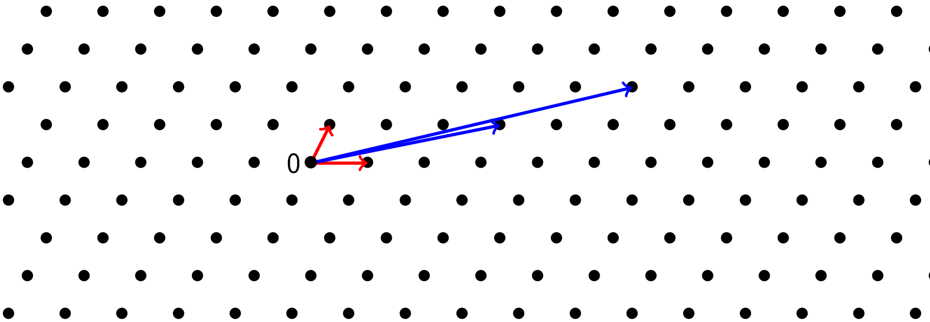
Heuristic:

$$\Pr_{x \leftarrow I}(x \cdot I^{-1} \in \mathcal{S}) \approx \delta_S[\beta^n],$$

$\delta_S[\beta^n] = \frac{|\mathcal{S} \cap \{I \,|\, \mathcal{N}(I) \leq \beta^n\}|}{|\{I \,|\, \mathcal{N}(I) \leq \beta^n\}|}$ is the density of $\mathcal{S}$ (among ideals of norm $\leq \beta^n$)

Objective: prove the heuristic

Lattices

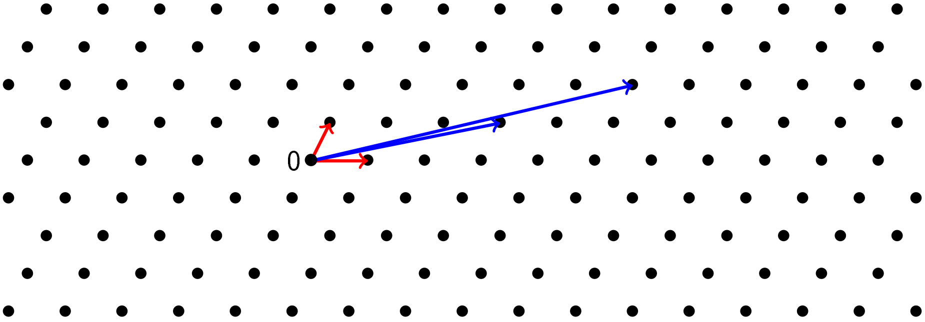


Lattice

A lattice L is a subset of $\mathbb{R}^n$ of the form $L = \{Bx \mid x \in \mathbb{Z}^n\}$, with $B \in \mathbb{R}^{n \times n}$ invertible. B is a basis of L, and n is its rank.

$\begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 17 & 11 \\ 4 & 2 \end{pmatrix}$ are two bases of the above lattice.

Lattices



Lattice

A lattice L is a subset of $\mathbb{R}^n$ of the form $L = \{Bx \mid x \in \mathbb{Z}^n\}$, with $B \in \mathbb{R}^{n \times n}$ invertible. B is a basis of L, and n is its rank.

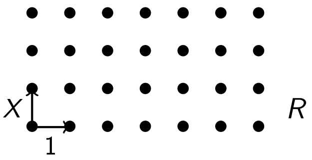
We represent a lattice by any of its basis

Ideals are lattices

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

(in fact, we actually use Minkowski's embedding)



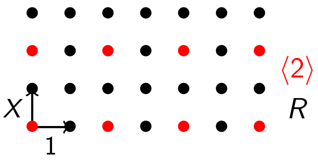
Ideals are lattices

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

(in fact, we actually use Minkowski's embedding)

$$\begin{cases} \langle g \rangle \subseteq R \simeq \mathbb{Z}^n \\ \text{stable by '+' and '-'} \end{cases} \Rightarrow \text{lattice}$$



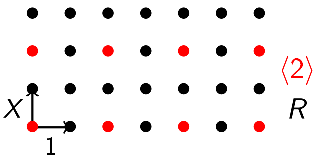
Ideals are lattices

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

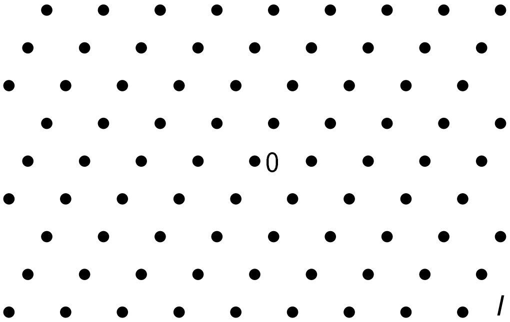
(in fact, we actually use Minkowski's embedding)

$$\begin{cases} \langle g \rangle \subseteq R \simeq \mathbb{Z}^n \\ \text{stable by '+' and '-'} \end{cases} \Rightarrow \text{ lattice}$$

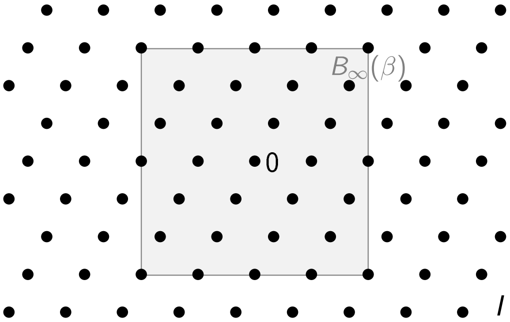


Conclusion: we have an embedding $K \to \mathbb{R}^n$ that maps ideals to lattices

Sampling x in I



Sampling x in I

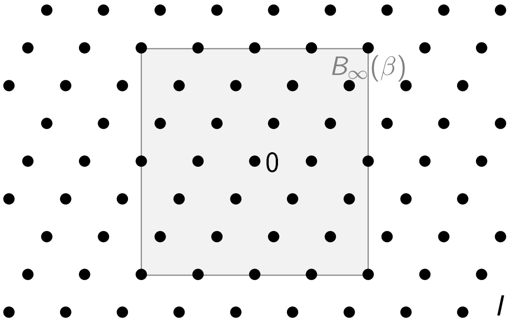


Distribution $\mathcal{D}_I$:

$$x \leftarrow \mathrm{Uniform}(I \cap B_\infty(\beta))$$

(previous works usually used Gaussian distributions)

Sampling x in I



Distribution $\mathcal{D}_I$:

$$x \leftarrow \mathrm{Uniform}(I \cap B_\infty(\beta))$$

(previous works usually used Gaussian distributions)

Efficiency: polynomial time if

$$\beta \geq 2^n$$

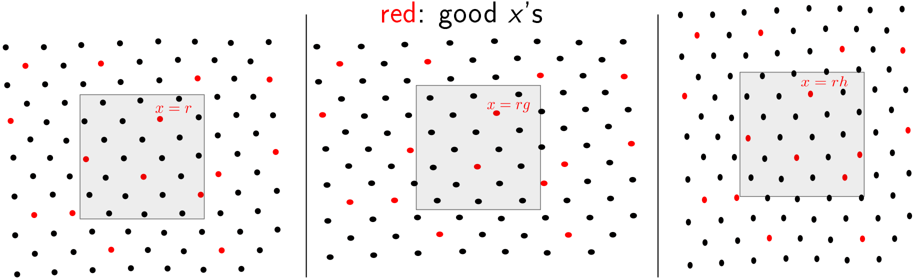
Proving the heuristic

Objective: $p_I := \Pr_{x \leftarrow \mathcal{D}_I}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$

Proving the heuristic

Objective: $p_I := \Pr_{x \leftarrow \mathcal{D}_I}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$

red: good x's

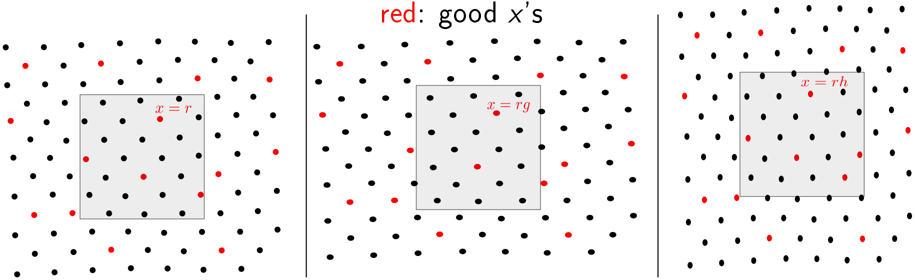


$I = R$ $\quad$ $I = \langle g \rangle$ $\quad$ $I = \langle h \rangle$

Proving the heuristic

Objective: $p_I := \Pr_{x \leftarrow \mathcal{D}_I}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$

red: good x's

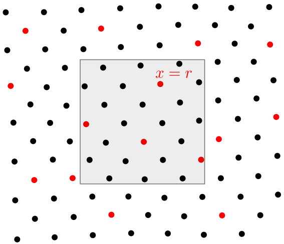


$I = R$	$I = \langle g \rangle$	$I = \langle h \rangle$
▸ $\langle x \rangle \cdot I^{-1} = \langle r \rangle$	▸ $\langle x \rangle \cdot I^{-1} = \langle r \rangle$	▸ $\langle x \rangle \cdot I^{-1} = \langle r \rangle$

Proving the heuristic

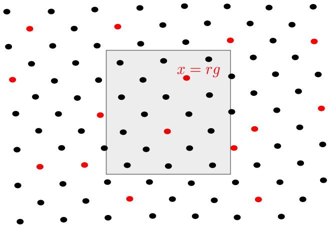
Objective: $p_I := \Pr_{x \leftarrow \mathcal{D}_I}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$

red: good x's



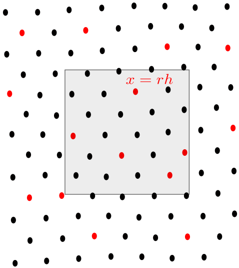
$I = R$

- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 4/24 = 1/6$



$I = \langle g \rangle$

- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 2/18 = 1/9$



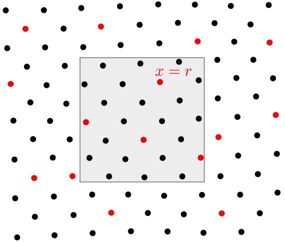
$I = \langle h \rangle$

- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 5/23$

Proving the heuristic

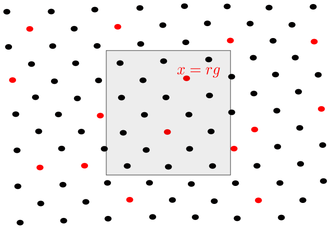
Objective: $p_I := \Pr_{x \leftarrow \mathcal{D}_I}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$

red: good x's



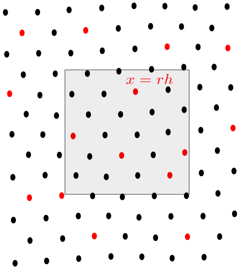
$I = R$

- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 4/24 = 1/6$



$I = \langle g \rangle$

- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 2/18 = 1/9$



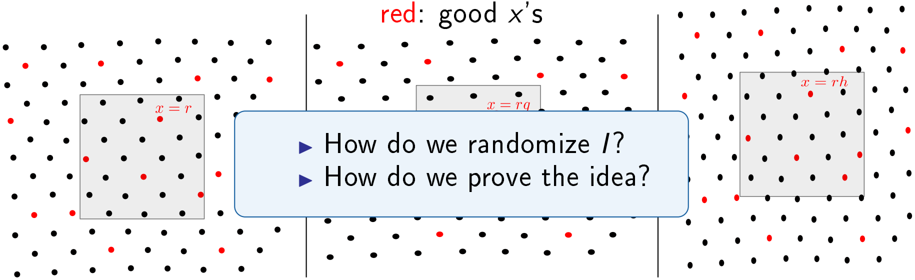
$I = \langle h \rangle$

- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 5/23$

Idea: Randomize the ideal $I \Rightarrow \Pr_{\substack{I \text{ random} \\ x \leftarrow \mathcal{D}_I}}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$

Proving the heuristic

Objective: $p_I := \Pr_{x \leftarrow \mathcal{D}_I}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$



- How do we randomize I?
- How do we prove the idea?

$I = R$
- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 4/24 = 1/6$

$I = \langle g \rangle$
- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 2/18 = 1/9$

$I = \langle h \rangle$
- $\langle x \rangle \cdot I^{-1} = \langle r \rangle$
- $p_I = 5/23$

Idea: Randomize the ideal $I \Rightarrow \Pr_{\substack{I \text{ random} \\ x \leftarrow \mathcal{D}_I}}\left(\langle x \rangle \cdot I^{-1} \in \mathcal{S}\right) \approx \delta_{\mathcal{S}}[\beta^n]$

A tool: the Log space

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^n \\ x &\mapsto (\log|x_1|, \cdots, \log|x_n|) \end{aligned}$$

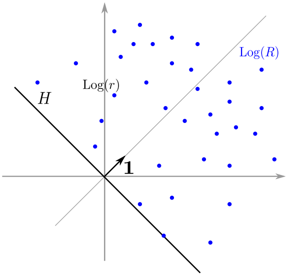
A tool: the Log space

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^n \\ x &\mapsto (\log|x_1|, \cdots, \log|x_n|) \end{aligned}$$

Properties

For all $r \in R$ and $x \in K$

- $\sum_i (\mathrm{Log}(r))_i \geq 0$



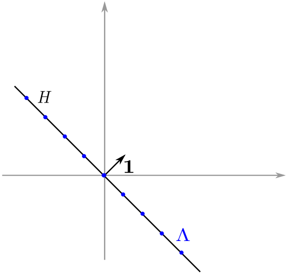
A tool: the Log space

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^n \\ x &\mapsto (\log|x_1|, \cdots, \log|x_n|) \end{aligned}$$

Properties

For all $r \in R$ and $x \in K$

- $\sum_i (\mathrm{Log}(r))_i \geq 0$
- $\sum_i (\mathrm{Log}(r))_i = 0$ iff r is a unit
- $\Lambda := \mathrm{Log}(R^\times)$ is a lattice



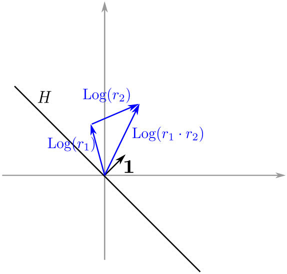
A tool: the Log space

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^n \\ x &\mapsto (\log|x_1|, \cdots, \log|x_n|) \end{aligned}$$

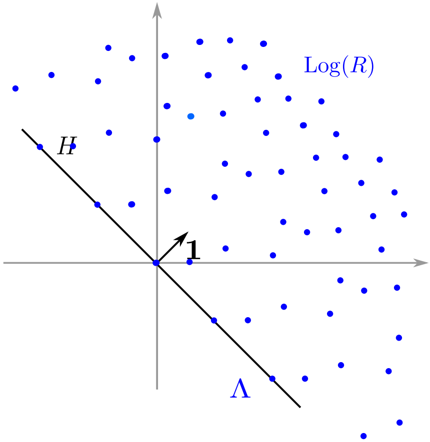
Properties

For all $r \in R$ and $x \in K$

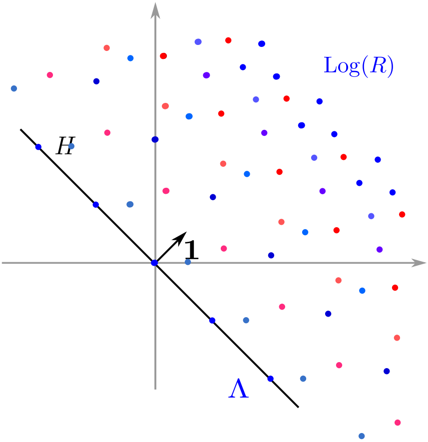
- $\sum_i (\mathrm{Log}(r))_i \geq 0$
- $\sum_i (\mathrm{Log}(r))_i = 0$ iff r is a unit
- $\Lambda := \mathrm{Log}(R^\times)$ is a lattice
- $\mathrm{Log}(r_1 \cdot r_2) = \mathrm{Log}(r_1) + \mathrm{Log}(r_2)$



What happens in the Log space

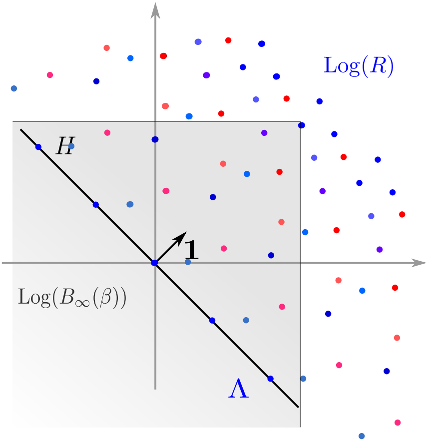


What happens in the Log space



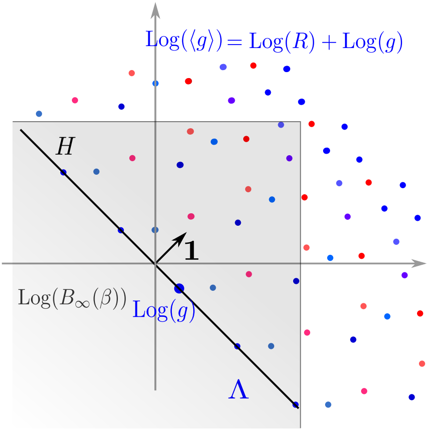
- red ●: good r's
  (i.e. $\langle r \rangle \in \mathcal{S}$)

What happens in the Log space



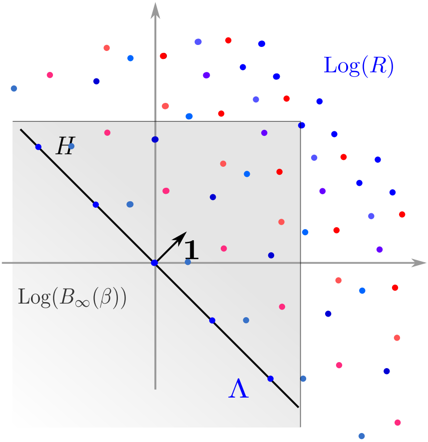
- red •: good r's (i.e. $\langle r \rangle \in \mathcal{S}$)
- $\mathrm{Log}(B_\infty(\beta)) = \{x \,|\, x_i \leq \log \beta\}$

What happens in the Log space



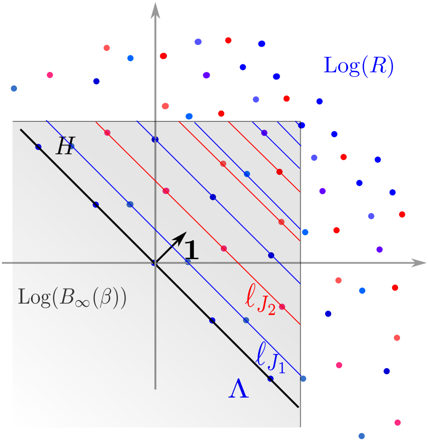
- red ●: good r's (i.e. $\langle r \rangle \in \mathcal{S}$)
- $\mathrm{Log}(B_\infty(\beta)) = \{x \mid x_i \le \log \beta\}$

What happens in the Log space



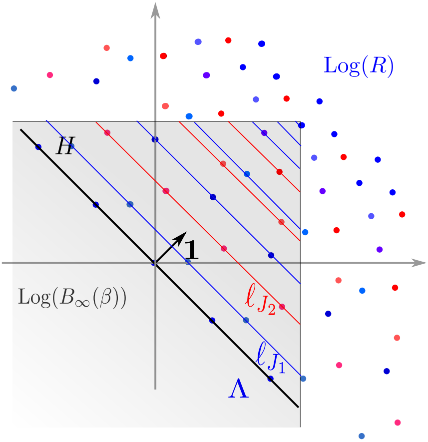
- red ●: good r's (i.e. $\langle r \rangle \in \mathcal{S}$)
- $\mathrm{Log}(B_\infty(\beta)) = \{x \mid x_i \leq \log \beta\}$

What happens in the Log space



- red ●: good r's (i.e. $\langle r\rangle \in \mathcal{S}$)
- $\mathrm{Log}(B_\infty(\beta)) = \{x \,|\, x_i \leq \log \beta\}$
- ℓ_J: length of line corresponding to J

What happens in the Log space

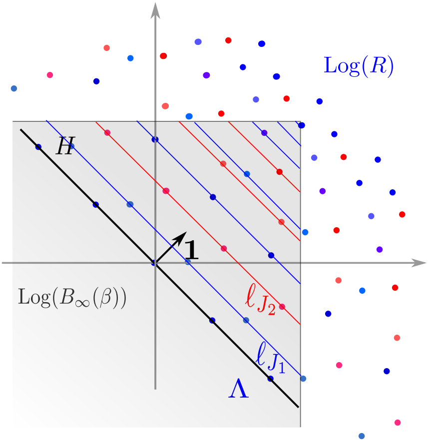


- red ●: good r's (i.e. $\langle r \rangle \in \mathcal{S}$)
- $\mathrm{Log}(B_\infty(\beta)) = \{x \mid x_i \le \log \beta\}$
- ℓ_J: length of line corresponding to J

$$\Pr_{\substack{g \leftarrow \mathcal{U}(H \bmod \Lambda) \\ x \leftarrow \mathcal{D}_{\langle g \rangle}}} \left(\langle x \cdot g^{-1} \rangle \in \mathcal{S} \right) = \frac{\sum_{\text{good J}} \ell_J}{\sum_{\text{all J}} \ell_J}$$

$$\delta_{\mathcal{S}}[\beta^n] = \frac{\sharp \text{ good J}}{\sharp \text{ all J}}$$

What happens in the Log space



- red ●: good r's (i.e. $\langle r\rangle \in \mathcal{S}$)
- $\mathrm{Log}(B_\infty(\beta)) = \{x \mid x_i \leq \log \beta\}$
- ℓ_J: length of line corresponding to J

$$\Pr_{\substack{g \leftarrow \mathcal{U}(H \bmod \Lambda) \\ x \leftarrow \mathcal{D}_{\langle g \rangle}}} \left(\langle x \cdot g^{-1}\rangle \in \mathcal{S}\right) = \frac{\sum_{\text{good J}} \ell_J}{\sum_{\text{all J}} \ell_J} \approx \frac{1}{3} \cdot \delta_{\mathcal{S}}[\beta^n] = \frac{\sharp \text{ good J}}{\sharp \text{ all J}}$$

Randomizing the ideal I

Theorem [BDPW20]

For some $N = \widetilde{O}(n)$ and $B = \mathrm{poly}(n)$, let $\mathcal{P}_B = \{\mathfrak{p} \text{ prime} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$.
Let I be any ideal and let $\mathfrak{p}_i \xleftarrow{\$} \mathcal{P}_B$, then

$$J = I \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_N$$

is uniformly random (i.e., $J = \langle g \rangle$, where $g \leftarrow \mathcal{U}(H \bmod \Lambda)$).

(actually, we also need a small distortion on the space)

[BDPW20] de Boer, Ducas, Pellet-Mary and Wesolowski. Random self-reducibility of ideal-SVP via Arakelov random walks. Crypto.

Summary

Algorithm: Given an ideal I

- Randomize the ideal: $J = I \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_N$, with $\mathfrak{p}_i \xleftarrow{\$} \mathcal{P}_B$
- Sample $x \xleftarrow{\$} J \cap B_\infty(2^n)$
- Repeat until $x \cdot J^{-1} \in \mathcal{S}$.

Summary

Algorithm: Given an ideal I

- Randomize the ideal: $J = I \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_N$, with $\mathfrak{p}_i \xleftarrow{\$} \mathcal{P}_B$
- Sample $x \xleftarrow{\$} J \cap B_\infty(2^n)$
- Repeat until $x \cdot J^{-1} \in \mathcal{S}$.

/!\ we ensure $x \cdot J^{-1} = x \cdot I^{-1} \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_N^{-1} \in \mathcal{S}$

Summary

Algorithm: Given an ideal I

- Randomize the ideal: $J = I \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_N$, with $\mathfrak{p}_i \xleftarrow{\$} \mathcal{P}_B$
- Sample $x \xleftarrow{\$} J \cap B_\infty(2^n)$
- Repeat until $x \cdot J^{-1} \in \mathcal{S}$.

/!\ we ensure $x \cdot J^{-1} = x \cdot I^{-1} \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_N^{-1} \in \mathcal{S}$

Our main theorem

Let x be sampled as in the algorithm above (without the rejection step). Let $\mathcal{S}_B$ be the set of B-smooth ideals. Then

$$\Pr_x(x \cdot I^{-1} \in \mathcal{S} \cdot \mathcal{S}_B) \geq \frac{1}{3}\delta_{\mathcal{S}}[2^{n^2}] - 2^{-n}.$$

(Need a small distortion in the algorithm + definition of $\delta_{\mathcal{S}}$ slightly different)

Outline of the talk

Computing units: general idea

Algorithm:

- Fix a bound B and a factor base $\mathcal{P}_B = \{\mathfrak{p} \text{ prime} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$

Nice survey: A. Gélin. Class group computations in number fields and applications to cryptology. Thèse de doctorat.

Computing units: general idea

Algorithm:

- Fix a bound B and a factor base $\mathcal{P}_B = \{\mathfrak{p} \text{ prime} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$
- Find relations $\langle g_j \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p},j}}$ (with g_j and the $\alpha_{\mathfrak{p},j}$ known)

Nice survey: A. Gélin. Class group computations in number fields and applications to cryptology. Thèse de doctorat.

Computing units: general idea

Algorithm:

- Fix a bound B and a factor base $\mathcal{P}_B = \{\mathfrak{p} \text{ prime} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$
- Find relations $\langle g_j \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p},j}}$ (with g_j and the $\alpha_{\mathfrak{p},j}$ known)
- Linear algebra: find $(y_j)_j$ such that $\sum_j y_j \alpha_{\mathfrak{p},j} = 0$ for all $\mathfrak{p} \in \mathcal{P}_B$
  ($\prod_j \langle g_j \rangle^{y_j} = \prod_{\mathfrak{p}} \mathfrak{p}^{\sum_j y_j \alpha_{\mathfrak{p},j}} = R$)

Nice survey: A. Gélin. Class group computations in number fields and applications to cryptology. Thèse de doctorat.

Computing units: general idea

Algorithm:

- Fix a bound B and a factor base $\mathcal{P}_B = \{\mathfrak{p} \text{ prime} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$
- Find relations $\langle g_j \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p},j}}$ (with g_j and the $\alpha_{\mathfrak{p},j}$ known)
- Linear algebra: find $(y_j)_j$ such that $\sum_j y_j \alpha_{\mathfrak{p},j} = 0$ for all $\mathfrak{p} \in \mathcal{P}_B$
  $(\prod_j \langle g_j \rangle^{y_j} = \prod_{\mathfrak{p}} \mathfrak{p}^{\sum_j y_j \alpha_{\mathfrak{p},j}} = R)$
- Output $\prod_j g_j^{y_j}$

Nice survey: A. Gélin. Class group computations in number fields and applications to cryptology. Thèse de doctorat.

Computing units: general idea

Algorithm:

- Fix a bound B and a factor base $\mathcal{P}_B = \{\mathfrak{p} \text{ prime} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$
- Find relations $\langle g_j \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p},j}}$ (with g_j and the $\alpha_{\mathfrak{p},j}$ known)
- Linear algebra: find $(y_j)_j$ such that $\sum_j y_j \alpha_{\mathfrak{p},j} = 0$ for all $\mathfrak{p} \in \mathcal{P}_B$
  $(\prod_j \langle g_j \rangle^{y_j} = \prod_{\mathfrak{p}} \mathfrak{p}^{\sum_j y_j \alpha_{\mathfrak{p},j}} = R)$
- Output $\prod_j g_j^{y_j}$

Run time: $\mathrm{poly}(B) \cdot T_{\text{relation}}$
(T_{relation}: time to find a relation)

Nice survey: A. Gélin. Class group computations in number fields and applications to cryptology. Thèse de doctorat.

Computing units: general idea

Algorithm:

- Fix a bound B and a factor base $\mathcal{P}_B = \{\mathfrak{p} \text{ prime} \,|\, \mathcal{N}(\mathfrak{p}) \leq B\}$
- Find relations $\langle g_j \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p},j}}$ (with g_j and the $\alpha_{\mathfrak{p},j}$ known)
- Linear algebra: find $(y_j)_j$ such that $\sum_j y_j \alpha_{\mathfrak{p},j} = 0$ for all $\mathfrak{p} \in \mathcal{P}_B$
  ($\prod_j \langle g_j \rangle^{y_j} = \prod_{\mathfrak{p}} \mathfrak{p}^{\sum_j y_j \alpha_{\mathfrak{p},j}} = R$)
- Output $\prod_j g_j^{y_j}$

Run time: $\mathrm{poly}(B) \cdot T_{\text{relation}}$
(T_{relation}: time to find a relation)

Nice survey: A. Gélin. Class group computations in number fields and applications to cryptology. Thèse de doctorat.

Finding relations

Objective

Find g and $\alpha_{\mathfrak{p}}$ such that $\langle g \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$

Finding relations

Objective

Find g and $\alpha_{\mathfrak{p}}$ such that $\langle g \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$

Algorithm

- Sample g randomly in R
- Repeat until $\langle g \rangle$ is B-smooth

Finding relations

Objective

Find g and $\alpha_{\mathfrak{p}}$ such that $\langle g \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$

Algorithm

- Sample g randomly in R
- Repeat until $\langle g \rangle$ is B-smooth

$\Rightarrow$ Heuristic

Finding relations

Objective

Find g and $\alpha_{\mathfrak{p}}$ such that $\langle g \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$

Algorithm

- Sample $I = \mathfrak{p}_1 \cdots \mathfrak{p}_N$, with $\mathfrak{p}_i \xleftarrow{\$} \mathcal{P}_B$
- Sample g randomly in I
- Repeat until $\langle g \rangle$ is B-smooth

$\Rightarrow$ Proven

Finding relations

Objective

Find g and $\alpha_{\mathfrak{p}}$ such that $\langle g \rangle = \prod_{\mathfrak{p} \in \mathcal{P}_B} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$

Algorithm

- Sample $I = \mathfrak{p}_1 \cdots \mathfrak{p}_N$, with $\mathfrak{p}_i \xleftarrow{\$} \mathcal{P}_B$
- Sample g randomly in I
- Repeat until $\langle g \rangle$ is B-smooth

$\Rightarrow$ Proven

$$T_{\text{relation}} \approx 3/\delta_{\mathcal{S}_B}[2^{n^2}] \approx \frac{\sharp\{I \mid \mathcal{N}(I) \leq 2^{n^2}\}}{\sharp\{B\text{-smooth ideal } I \mid \mathcal{N}(I) \leq 2^{n^2}\}}$$

What we still need…

… to fully prove the algorithm

What we still need. . .

. . . to fully prove the algorithm

- An effective lower bound on $\delta_{\mathcal{S}_B}[2^{n^2}]$

What we still need. . .

. . . to fully prove the algorithm

- An effective lower bound on $\delta_{\mathcal{S}_B}[2^{n^2}]$
- A way to prove that the relations we create are independent
  (if we want to find all units)

Conclusion

- Some things that were partially hidden:
  - the result also holds for non-principal domains R
  - need to distort slightly the box $B_\infty(2^n)$

Conclusion

- Some things that were partially hidden:
  - the result also holds for non-principal domains R
  - need to distort slightly the box $B_\infty(2^n)$
- This is a result to prove heuristics
  - Can we remove all heuristics of [BF14] and/or [BP17]?
    (Koen is working on it)

Conclusion

- Some things that were partially hidden:
  - the result also holds for non-principal domains R
  - need to distort slightly the box $B_\infty(2^n)$
- This is a result to prove heuristics
  - Can we remove all heuristics of [BF14] and/or [BP17]?
    (Koen is working on it)

Questions?