LFANT seminar — 24 janvier 2023

The particular case of cyclotomic fields when computing unit groups by quantum algorithms

Razvan Barbulescu
CNRS, Institut de mathémathiques de Bordeaux

Joint work with:

Adrien Poulalion
(X, Corps des Mines)

Plan of the talk

- Reducing the unit group computations to the hidden subgroup problem
- The continuous hidden subgroup problem
- The particular case of cyclotomic fields

Shor's algorithms (1/2)

Hidden subgroup problem (HSP) and its continuous version (CHSP)

- HSP. Assume that $f : \mathbb{Z}^m \to \mathbb{C}^k$ is such that there exists a lattice $L \subset \mathbb{Z}^n$,

$$\forall \ell \in L, \quad f(x+\ell) = f(x).$$

  Given an algorithm to compute f, find L.
- CHSP : same definition with $f : \mathbb{R}^m \to \mathbb{C}^k$ and additional conditions on f.

History of HSP in quantum algorithms for number theory

- 1994 Simon : polynomial time quantum algorithm to solve HSP
- 1994 Shor : reduce factoring and DLP in abelian groups to HSP
- ...

Shor's algorithms (2/2)

Shor's factoring and DLP algorithms

- When factoring N, take a random $a \in (\mathbb{Z}/N)^*$. The period of $\left(\begin{array}{cccc} f: & \mathbb{Z} & \to & \mathbb{C} \\ & i & \mapsto & a^i \end{array}\right)$ is the order of a and, with high probability, the order of $(\mathbb{Z}/N)^*$.
  - If $N = pq$, knowing the order $(p-1)(q-1)$ of $(\mathbb{Z}/N)^*$ is equivalent to knowing p and q. For general N,
  - Bach gave a probabilitic reduction.
- Assume every element of a group G is represented by an element of $\mathbb{C}^k$. When computing $\log_g h$, the function $\left(\begin{array}{cccc} f: & \mathbb{Z}^2 & \to & \mathbb{C}^k \\ & (i,j) & \mapsto & g^i h^j \end{array}\right)$ has as period set the lattice generated by $(\#G, 0)$, $(0, \#G)$ and $(\log_g h, -1)$.

History

History of HSP in quantum algorithms for number theory

- 1994 Simon: polynomial time quantum algorithm to solve HSP
- 1994 Shor: reduce factoring and DLP in abelian groups to HSP
- 2002 Hallgren: reduce $\mathcal{O}_K^*$ when K is quadratic real to CHSP with $n = 2$
- 2005 Schmidt and Vollmer $\|$ Hallgren: reduce $\mathrm{Cl}(K)$ in fixed degree to HSP
- 2014 Eisenträger, Hallgren, Kitaev, Song: reduce $\mathcal{O}_K^*$ to CHSP
- 2014 Campbel, Groves, Shepherd (Soliloquy): non peer-reviewed claim to reduce $\mathrm{Cl}(K)$ of arbitrary degree to HSP
- 2014 Bernstein: blog post stating that the Soliloquy talk was false
- 2015 Biasse and Song: proof that the reduction of $\mathrm{Cl}(K)$ to HSP is false
- 2016 Biasse and Song: reduction of $\mathrm{Cl}(K)$ to CHSP
- 2019 den Boer, Ducas, Fehr: complete proof that CHSP is quantum polynomial time and precise analysis of qubits requirements

History

History of HSP in quantum algorithms for number theory

- 1994 Simon: polynomial time quantum algorithm to solve HSP
- 1994 Shor: reduce factoring and DLP in abelian groups to HSP
- ~~2002~~ 2007 Hallgren: reduce $\mathcal{O}_K^*$ when K is quadratic real to CHSP with $n = 2$
- 2005 Schmidt and Vollmer ∥ Hallgren: reduce $\mathrm{Cl}(K)$ in fixed degree to HSP
- ~~2014~~ 2019 Eisenträger, Hallgren, Kitaev, Song: reduce $\mathcal{O}_K^*$ to CHSP and CHSP
- ~~: non peer-reviewed claim to reduce $\mathrm{Cl}(K)$ of arbitrary degree to HSP~~
- ~~2014 Bernstein: blog post stating that the above claim is false~~
- ~~2015~~ 2019 Biasse and Song: proof that the reduction of $\mathrm{Cl}(K)$ to HSP is false
- 2016 Biasse and Song: reduction of $\mathrm{Cl}(K)$ to CHSP
- 2019 den Boer, Ducas, Fehr: complete proof that CHSP is quantum polynomial time and precise analysis of qubits requirements

History

History of HSP in quantum algorithms for number theory

- 1994 Simon: polynomial time quantum algorithm to solve HSP
- 1994 Shor: reduce factoring and DLP in abelian groups to HSP
- ~~2002~~ 2007 Hallgren: reduce $\mathcal{O}_K^*$ when K is quadratic real to CHSP with $n = 2$
- 2005 Schmidt and Vollmer $\|$ Hallgren: reduce $\mathrm{Cl}(K)$ in fixed degree to HSP
- ~~2014~~ 2019 Eisenträger, Hallgren, Kitaev, Song: reduce $\mathcal{O}_K^*$ to CHSP and CHSP
- ~~: non peer-reviewed claim to reduce $\mathrm{Cl}(K)$ of arbitrary degree to HSP~~
- ~~2014 Bernstein: blog post stating that the above claim is false~~
- ~~2015~~ 2019 Biasse and Song: proof that the reduction of $\mathrm{Cl}(K)$ to HSP is false
- 2016 Biasse and Song: reduction of $\mathrm{Cl}(K)$ to CHSP
- 2019 den Boer, Ducas, Fehr: complete proof that CHSP is quantum polynomial time and precise analysis of qubits requirements

$\boxed{\text{den Boer et al. proposed a list of open questions}}$

Plan of the talk

- Reducing the unit group computations to the hidden subgroup problem
- The continuous hidden subgroup problem
- The particular case of cyclotomic fields

Some definitions on lattices

Definitions

- $\mathrm{SVP}(L)$: the problem of finding the shortest vector;
- λ_1 is the lenght of the shortest vector b_1, for $k \geq 1$, λ_{k+1} is the lenght of the shortest vector b_k not spanned by $(b_1, \ldots, b_k)$;
- $\mathrm{CVP}(x, L)$: the problem of finding the closes vector;
- $\mathrm{BDD}(x, L, \delta\lambda_1)$: it is CVP with the promise to be at distance $\delta\lambda_1$ from the lattice.

Some properties of lattices

Complexity

- SVP and CVP are believed exponential time on classical and quantum computers
- Babai (1985) solves BDD in polynomial time when δ is very small, but in general it is exponential time.

Canonical basis

- There is no canonical basis of a lattice, so one cannot apply period-finding algorithms if the image is a lattice.
- **Lemma:** When $\dim L = 2$, let v_1 and v_2 be such that $\|v_i\| = \lambda_i$. Then the datum (v_1, v_2) is a canonical representation and can be computed in polynomial time using Gauss' algorithm.
- in a general lattice L of dimension n, the vectors of lenght $\lambda_1, \ldots, \lambda_n$ are unique up to sign. This suggests a unique representation of lattices in $\mathbb{C}^{n^2}$ but it requires to solve SVP.
- Hence $\mathrm{Cl}(K)$ and $\mathcal{O}_K^*$ are easier in fixed degree n because one has canonical representations of lattices of $\mathbb{R}^n$.

Prerequisites about lattices

Definition and properties of the dual of a lattice

- $L^* := \{y \in \mathbb{R}^m \mid \forall x \in L, x \cdot y \in \mathbb{Z}^n\}$;
- $\lambda_1^* := \lambda_1(L^*)$
- if L is generated by the rows of a matrix B then L^* is generated by the rows of $(B^t)^{-1}$; in particular $\det L^* = 1/\det L$;
- if $M \subset L$ then $L^* \subset M^*$ and $[L : M] = [M^* : L^*]$.

Modeling the quantum part of the algorithm

Definition (Dual lattice sampler)

Let $c : L^* \to \mathbb{C}$ be a map such that $\sum_{\ell^*\in L^*} |c_{\ell^*}|^2 = 1$. Let ϵ and δ be two parameters. An algorithm is a dual lattice sampler of parameters $1/4 > \eta > 0$ and $1/2 > \delta > 0$ if it outputs a vector $x \in \mathbb{R}^m$ such that, for any finite set $S \subset L^*$, one has

$$\mathrm{Prob}\left(y \in \bigcup_{\ell^*\in S} B(\ell^*, \delta\lambda_1^*) \right) \geq \sum_{\ell^*\in S} |c_{\ell^*}|^2 - \eta.$$

It means morally that the probability of drawing a vector close to $l^* \in L^*$ is approximately $|c_{\ell^*}|^2$: these quantities act as a probability distribution. We add also two technical conditions for the map c:

1. **Uniformity property** : there exists $\varepsilon \leq 1/4$ such that, for every strict sublattice $N \subsetneq L^*$:
$$\sum_{\ell^*\in N} |c_{\ell^*}|^2 < \frac{1}{2} + \varepsilon.$$
2. **Concentration property** : There exists $R = R(m)$ and $0 < p < \frac{1}{2} - \varepsilon - \eta$ such that :
$$\sum_{|\ell^*|>R} |c_{\ell^*}|^2 < p.$$

Preparation: random vectors to generate a lattice

Examples

- Bost and Mestre (1988) : complex AGM to compute periods in genus 1 and 2
- Hafner and Buchmann (1989) : classical class group
- den Boer et al. (2019) : CHSP

Lemma (dBDF 2019)

We note $k = \alpha(m + m\log_2 R + \log_2(\det L))$, for an absolute constant $\alpha > 1$. Let $\widetilde{y}_1, \widetilde{y}_2, \ldots, \widetilde{y}_k$ be the first k vectors output by a dual basis sampler. For $i = \overline{1,k}$ put $y_i = \mathrm{CVP}(\widetilde{y}_i, L)$. Then for any value of the absolute constant $\alpha > 2$ we have

$$\mathrm{Prob}(y_1, \ldots, y_k \text{ generate } L) \geq 1 - c^m,$$

where $c < 1$ is an explicitly computable constant.

The CHSP algorithm

Input τ and approximations at one bit of precision of R, λ_1^* and $\det L$;
Output a basis of L with absolute error τ

1: $k \leftarrow m \log_2 R - \log_2(\det L))$; $\delta = \frac{(\lambda_1^*)^2 \det L^*}{2^{O(mk)} \|B\|_\infty^{m+1}} \tau$
2: **for** $i = 1, 2, \ldots, k$ **do** ▷ Step 1 - Quantum
3: $\quad \widetilde{y_i} \leftarrow$ output(dual lattice sampler(δ))
4: $\quad$ pass
5: **end for**
6: Use Buchmann-Pohst algorithm on $(\widetilde{y_1}, \ldots, \widetilde{y_k})$ to find a basis $(y_1, \ldots, y_m)$ of L^*; call B the square matrix they form ▷ Step 2 - Classical
7: Output $(B^{-1})^t$ (here B is the matrix a basis of L^*). ▷ Step 3 - Classical

Buchmann-Pohst: extract a basis from the approximation of a generating set (1/3)

The case $\dim L = 1$: given $\widetilde{k\alpha}$ and $\widetilde{\ell\alpha}$ with absolute error δ, find $\alpha \in \mathbb{R}$

- Theorem (Dirichlet): For any $\beta \in \mathbb{R} \backslash \mathbb{Q}$ there exists a sequence $(p_n, q_n)_n$ such that $q_n \to \infty$ and
$$\left| \beta - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$
- Let p/q be a Dirichlet approximation of $\widetilde{k\alpha}/\widetilde{\ell\alpha}$. Put $\delta_k := |k\alpha - \widetilde{k\alpha}|$ and similarly for δ_ℓ. If $\max(\delta_k, \delta_\ell) < \frac{1}{\alpha(p+q)}$ and $q \geq \ell$ then
$$p/q = k/\ell.$$
Indeed,
$$\left| \frac{k\alpha + \delta_k}{\ell\alpha + \delta_\ell} - \frac{p}{q} \right| < \frac{1}{q^2}$$
implies that $\frac{1}{q^2} > \frac{kq - p\ell}{q\ell}$, which is possible only if $kq - p\ell = 0$.

Buchmann-Pohst: extract a basis from the approximation of a generating set (2/3)

The general case

$$\begin{pmatrix} \boxed{\lfloor \widetilde{b_1} 2^q \rfloor} & \cdots & \boxed{\lfloor \widetilde{b_k} 2^q \rfloor} \\ 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \leadsto^{\mathrm{LLL}} \left(\begin{array}{ccc|ccc} \boxed{\varepsilon_1} & \cdots & \boxed{\varepsilon_{k-n}} & \boxed{\widetilde{c_1}} & \cdots & \boxed{\widetilde{c_n}} \\ m_{1,1} & & m_{n,1} & & & \\ \vdots & & \vdots & & \star & \\ m_{1,k} & & m_{n,k} & & & \end{array}\right)$$

Theorem (Buchmann-Pohst)

If $q \geq q(L)$, an explicite expression depending only on L, the LLL-reduction of the above matrix is such that

- $\varepsilon_1, \ldots, \varepsilon_{k-n}$ *have norm bounded by an explicit constant;*
- $m_1, \ldots, m_{k-n} \in L^*$
- $2^{-q}(\widetilde{c_1}, \ldots, \widetilde{c_n})$ *is a an approximation of a basis of L.*

Buchmann-Pohst: extract a basis from the approximation of a generating set (3/3)

The particular case of $\mathbb{Q}(\zeta_n)$ when $4 \mid \varphi(n)$

- $\mathcal{O}_K^*$ is a $\mathbb{Z}[\mathrm{Gal}(K)]$-module, in particular a $\mathbb{Z}[i]$-module
- Poulalion: Buchmann-Pohst extends to $\mathbb{Z}[i]$

LLL over $\mathbb{Z}$ vs. LLL over $\mathbb{Z}[i]$

- Fieker-Stehlé (2010): to reduce a $\mathbb{Z}[i]$-module one can forget the $\mathbb{Z}[i]$-structure, $\mathbb{Z}$-reduce and retrieve the $\mathbb{Z}[i]$-structure;
- Kim-Lee (2017): LLL over $\mathbb{Z}[\zeta_k]$ works in practice even when $\mathbb{Z}[\zeta_k]$ is not Euclidean;
- Camus (2018): implementation of LLL over $\mathbb{Z}[i]$ faster than the best implementation of LLL over $\mathbb{Z}$.

Space complexity of CHSP (1/2)

Definition (Continuous Hidden Subgroup Problem - CHSP)

Let $f : \mathbb{R}^m \to \mathcal{S}$, where $\mathcal{S} = \oplus_{i\in\{0,1\}^n}\mathbb{C}|i\rangle$ is the space of states of n qubits.
The function f is **an** (a, r, ε)**-oracle hiding the full-rank lattice** L if and only if it verifies the following technical conditions:

1. L is the period of f, i.e. $\forall x \forall \ell \in L, f(x+\ell) = f(x)$. (periodicity)
2. The function f is a-Lipschitz. (Lipschitz condition)
3. $\forall x, y \in \mathbb{R}^m$ such that $dist(x-y, L) \geq r$, we have $|\langle f(x) \mid f(y)\rangle| \leq \varepsilon$. (strong periodicity)

Given an efficient quantum algorithm to compute f, compute the hidden lattice of periods L.

Representing a lattice in $\mathbb{C}^k$ with $k < \infty$ (EHKS 2014)

- (straddle encoding):
  $|\mathrm{str}_\nu(x)\rangle = \cos(\frac{\pi}{2}t)|k\rangle + \sin(\frac{\pi}{2}t)|k+1\rangle$, where $k = \lfloor x/\nu \rfloor$, $t = x/\nu - k$
- $|\mathrm{str}_{n,\nu}(x_1, \ldots, x_n)\rangle = \otimes_{i=1}^n |\mathrm{str}_\nu(x_i)\rangle$
- $f(L) = \gamma^{-1/2} \sum_{x\in L} e^{-\pi\|x\|^2/s} |\mathrm{str}_{n,\nu}(x)\rangle$ with $\gamma = \sum_{x\in L} e^{-2\pi\|x\|^2/s^2}$.

Space complexity of CHSP (2/2)

Theorem (dBDF 2019)

CHSP can be solved with a quantum algorithm with the following complexities:

- *time:* $O(km^2Q^2)$
- *space:* $mQ + n$ *with*

$$\begin{aligned} Q &= O(mk) + O(\log \tfrac{a}{\lambda_1^*}) + O(\log \tfrac{1}{\lambda_1^* \tau}), \\ k &= O(m \log(\sqrt{m} a (\det L)^{1/m})). \end{aligned}$$

k is the expectancy of the number of random vectors to generate L^*.

Reduction of the $\mathcal{O}_K^*$ computation to CHSP (1/2)

Lemma (The example of totally real fields)

Let $K \subset \mathbb{R}$ be an embedding of K. Then the function $\left(\begin{array}{cccc} f: & \mathbb{R} & \to & \mathcal{P}(\mathbb{R}) \\ & x & \mapsto & e^x\mathcal{O}_K \end{array}\right)$ *has the period* $\log \mathcal{O}_K^*$.

Proof.

$$\begin{aligned} e^x\mathcal{O}_K = e^y\mathcal{O}_K &\Leftrightarrow e^{x-y}\mathcal{O}_K = \mathcal{O}_K \\ &\Leftrightarrow e^{x-y} \in K \text{ and } \langle e^{x-y}\rangle = \mathcal{O}_K \\ &\Leftrightarrow \pm(x-y) \in \log(\mathcal{O}_K^*) \end{aligned}$$

□

Reduction of the $\mathcal{O}_K^*$ computation to CHSP (1/2)

Lemma (The example of totally real fields)

Let $K \subset \mathbb{R}$ be an embedding of K. Then the function $\begin{pmatrix} f: & \mathbb{R} & \to & \mathcal{P}(\mathbb{R}) \\ & x & \mapsto & e^x\mathcal{O}_K \end{pmatrix}$ *has the period* $\log \mathcal{O}_K^*$.

Modify f to be used in CHSP

- $\log \mathcal{O}_K^*$ is not discret (not a lattice). Let $K \subset \mathbb{R}$ be an embedding and set $\sigma_1 = \mathrm{id}$. Let σ_1, σ_{r_1} be field automorphisms of $\mathbb{R}$ which extend the real embeddings of K and let $\tau_{r_1+i}, \overline{\tau_{r_1+1}}, \ldots$ be some complex embeddings of $\mathbb{R}$ which extend the complex embeddings of K. Put $\sigma_{r_1+i} = \sqrt{|\tau_{r_1+i}|}$ and $r = r_1 + r_1 - 1$. $\begin{pmatrix} f: & \mathbb{R}^{r_1+r_2} & \to & \mathcal{P}(\mathbb{R})^{r+1} \\ & (x_1, x_2, \ldots, x_{r+1}) & \mapsto & (e^{x_1}\sigma_1(\mathcal{O}_K), e^{x_2}\sigma_2(\mathcal{O}_K), \ldots, e^{x_{r+1}}\sigma_{r+1}(\mathcal{O}_K)) \end{pmatrix}$ has the period $\log \mathcal{O}_K^*$.
- encode any lattice of $\mathbb{R}^{r+1}$, e.g. $e^x\mathcal{O}_K$, by $\mathbb{R}^q \subset \mathbb{C}^q$ for a large enough q.

One actually finds $\{u\overline{u} \mid u \in \mathcal{O}_K^*\}$

- if only wants the regulator or $\mathcal{O}_K^*/(\mathcal{O}_K^*)^\ell$ for a large primeℓ then we are done.
- For all $\mathcal{O}_K^*$ use n embeddings. For the roots of unity one factors the discriminant.[a]

[a] Eisenträger et al. prove that if F has domain $G \times \mathbb{Z}^k \times \mathbb{R}^m$ and is continuous on $\mathbb{R}^m$ one can construct a continuous function whose period is the same. (HSP reduces to CHSP)

Space complexity of the algorithm for $\mathcal{O}_K^*$

EHKS 2014 long version (2019)

- $m = O(n)$ and $n = O(m)$ where $n = \deg K$
- Theorem 5.5 and D.4: f is an $(a = \sqrt{\pi/4}c(\sqrt{m}/\lambda_1)^n + 1, R = O(m^2 + m \log D), \varepsilon = 3/4)$-oracle for CHSP
- Theorem B.3: $\lambda_1 \geq 1/2$
- Equation (D.11): $\lambda_1^* = \Omega(1/\sqrt{m})$

Comparison between HSP and CHSP when computing $\mathcal{O}_K^*$

Notations: $m = O(n) = O(\deg K)$ and $D = \mathrm{disc} K$.

- When inserted in the dBDF space complexity we get

$$\text{space} = O(m^4 \log m + m^3 \log D + m \log \tau).$$

- For comparison, the space of HSP is dominated by that of HNF: Micianccio and Warinschi 2001 : $\mathrm{space}(\mathrm{HNF}) = O(m^2 \log D)$.

Question: can we find particular cases without Buchmann-Pohst ?

Plan of the talk

- Reducing the unit group computations to the hidden subgroup problem
- The continuous hidden subgroup problem
- The particular case of cyclotomic fields

Cyclotomic units

Definition

In $K=\mathbb{Q}(\zeta)$ with ζ an mth root of unity, the group of cyclotomic units is the subgroup C of $\mathcal{O}_K^*$ generated by the roots of unity and ζ_m^i-1 with $i\in\mathbb{N}$.

Properties whem $m=p^e$ (see e.g. Cramer, Ducas, Peikert, Regev 2015)

- (Whashington) C is generated by $\pm\zeta$ and

$$\beta_j := \frac{\zeta^j-1}{\zeta-1},$$

  with $j\in(\mathbb{Z}/m)^*/\{\pm1\}$, $j\neq 1$.
- (Whashington) $[\mathrm{Log}\mathcal{O}_K^* : \mathrm{Log}\, C] = h^+(m) := \mathrm{h}(\mathbb{Q}(\zeta+1/\zeta))$.
- (CDPR15)[a] We set $b_j=\mathrm{Log}\beta_j$ where $\mathrm{Log}=(\log\sigma_1,\log\sigma_2,\ldots,\log\sigma_n)$. Let $\{b_j^*\}_j$ be the dual basis of $\{b_j\}$. Then $\left\|b_j^*\right\|^2=\Omega(m^{-1}\log^3 m)$. and in particular

$$1/\lambda_1(M^*)=O(m/\log^3 m).$$

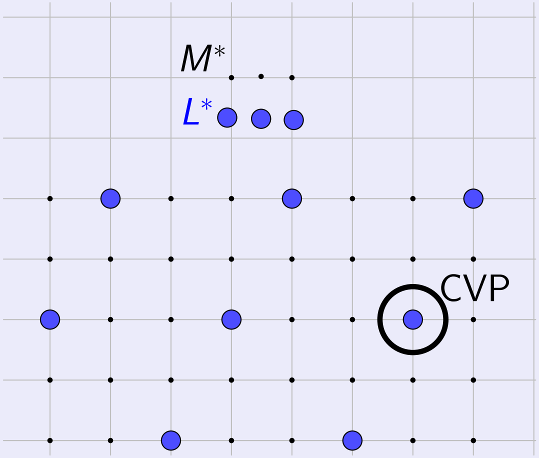
[a] Cramer, Ducas, Peikert, Regev (2015) only treat the case $m=p^e$ but the general can be treated as in Lemma 3.5 of Cramer ducas Wesolowski (2021).

$$\boxed{M:=\mathrm{Log}\, C \text{ is a sublatice of } L:=\mathrm{Log}\mathcal{O}_K^*}$$

The checker-corrector (1/2)

When CVP(M^*) brings points in L^*

$M \subset L$ so $L^* \subset M^*$

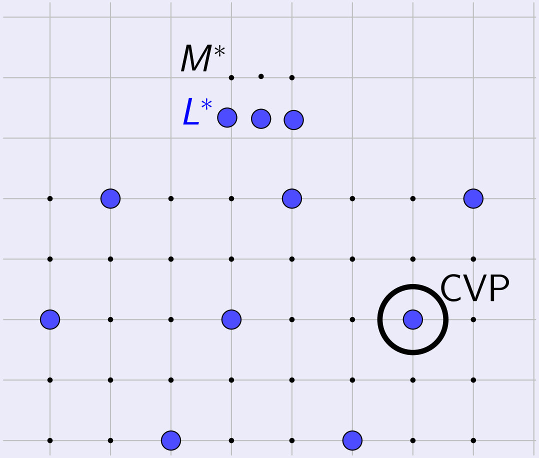


If $d(x, L^*) < \frac{1}{2}\lambda_1(M^*)$ then $\mathrm{CVP}(x, M^*)$ returns a point of L^*.

The checker-corrector (1/2)

When CVP(M^*) brings points in L^*

$M \subset L$ so $L^* \subset M^*$



If $d(x, L^*) < \frac{1}{2}\lambda_1(M^*)$ then $\mathrm{CVP}(x, M^*)$ returns a point of L^*.

Do the quantum part in low percision and correct it before Buchmann-Pohst.

The checker-corrector (2/2)

Lemma

Let $M \subset L$ be a lattice generated by B_M (a matrix for L is not necessarily known). If $\widetilde{y} \in \mathbb{R}^n$ is such that $d(\widetilde{y}, L^*) < \frac{1}{2}\lambda_1(M^*)$ then one can solve $\mathrm{CVP}(\widetilde{y}, L^*)$ in polynomial time.

Proof.

The following algorithm has a polynomial time complexity:

1. compute $\widetilde{z} := B_M^t \widetilde{y}$;
2. round $z = (z_1, \ldots, z_n) := (\lfloor \widetilde{z_1} \rceil, \ldots, \lfloor \widetilde{z_n} \rceil)$;[a]
3. return $y := (B_M^t)^{-1} z$.

The checker-corrector (2/2)

Lemma

Let $M \subset L$ be a lattice generated by B_M (a matrix for L is not necessarily known). If $\widetilde{y} \in \mathbb{R}^n$ is such that $d(\widetilde{y}, L^*) < \frac{1}{2}\lambda_1(M^*)$ then one can solve $\mathrm{CVP}(\widetilde{y}, L^*)$ in polynomial time.

Proof.

The following algorithm has a polynomial time complexity:

1. compute $\widetilde{z} := B_M^t \widetilde{y}$;
2. round $z = (z_1, \ldots, z_n) := (\lfloor \widetilde{z_1} \rceil, \ldots, \lfloor \widetilde{z_n} \rceil)$;[a]
3. return $y := (B_M^t)^{-1} z$.

$$\begin{aligned} \|y - \widetilde{y}\| &= \left\|(B_M^t)^{-1}(z - \widetilde{z})\right\| \\ &\leq \left\|(B_M^t)^{-1}\right\| \|z - \widetilde{z}\| = \|B_{M^*}\| \|z - \widetilde{z}\| \\ &\leq \lambda_1(M^*) \cdot \tfrac{1}{2}. \end{aligned}$$

Let $y_L = \mathrm{CVP}(\widetilde{y}, L^*)$. Then

$$\|y_L - y\| \leq \|y_L - \widetilde{y}\| + \|y - \widetilde{y}\| < \frac{1}{2}\lambda_1(M^*) + \frac{1}{2}\lambda_1(M^*) = \lambda_1(M^*).$$

Since $y_L \in L^* \subset M^*$, $y_L - y \in M^*$ so $y = y_L$. □

[a] If $d(\widetilde{y}, L^*) < \frac{1}{4}\lambda_1(M^*)$ and $\|z - \widetilde{z}\| > 1/4$ we can discard $\widetilde{y}$. The algoritms is a "checker".

Solving CHSP in the cyclotomic case

Input τ and approximations at one bit of precision of R, λ_1^* and $\det L$;
Output a basis of L with absolute error τ

1: $k \leftarrow m \log_2 R - \log_2(\det L)$; $\cancel{\delta = \frac{(\lambda_1^*)^2 \det L^*}{2^{O(mk)} \|B\|_\infty^{m+1}} \tau}$ $\delta = \frac{1}{2}\lambda_1(M^*)$
2: **for** $i = 1, 2, \ldots, k$ **do** ▷ Step 1 - Quantum
3: $\widetilde{y_i} \leftarrow$ output(dual lattice sampler(δ))
4: ~~pass~~ correct $(\widetilde{y_1}, \ldots, \widetilde{y_k})$ from error $\frac{1}{2}\lambda_1(M^*)$ to error $\frac{(\lambda_1^*)^2 \det L^*}{2^{O(mk)} \|B\|_\infty^{m+1}} \tau$
5: **end for**
6: Use Buchmann-Pohst algorithm on $(\widetilde{y_1}, \ldots, \widetilde{y_k})$ to find a basis $(y_1, \ldots, y_m)$ of L^*; call B the square matrix they form ▷ Step 2 - Classical
7: Output $(B^{-1})^t$ (here B is the matrix a basis of L^*). ▷ Step 3 - Classical

Space complexity of the quantum step

- **without the corrector:** From slide "Space complexity":

$$\text{space} - m \log \tau = O(m^4 \log m + m^3 \log D) = O(m^4 \log m) = \widetilde{O}(m^4)$$

  because $D = \mathrm{disc}(\mathbb{Q}(\zeta_m)) = O(m^m)$.

- **with the corrector:**

$$\text{space} - m \log \tau = O(m(\log \delta)) = O(m \log \lambda_1(M^*)) = O(m^2 / \log^3 m) = \widetilde{O}(m^2).$$

A different point of view

Input τ and approximations at one bit of precision of R, λ_1^* and $\det L$;
Output a basis of L with absolute error τ

$k \leftarrow m \log_2 R - \log_2(\det L))$; $\delta = \frac{(\lambda_1^*)^2 \det L^*}{2^{O(mk)} \|B\|_\infty^{m+1}} \tau$
for $i = 1, 2, \ldots, k$ **do** ▷ Step 1 - Quantum
    $\widetilde{y_i} \leftarrow$ output(dual lattice sampler(δ))
    ~~pass~~ correct $(\widetilde{y_1}, \ldots, \widetilde{y_k})$ with an error small enough to obtain $(y_1, \ldots, y_n)$ with integer coordinates in a basis of M^*.
end for
~~Use Buchmann-Pohst algorithm on $(\widetilde{y_1}, \ldots, \widetilde{y_k})$ to find a basis $(y_1, \ldots, y_m)$ of L^*;~~ Compute a Hermite normal form (HNF) to obtain the exact value of $[L : M]$. ▷ Step 2 - Classical
Output $(B^{-1})^t \in \frac{1}{[L:M]} \mathrm{Mat}_m(\mathbb{Z})$, where $B \in \mathrm{Mat}_m(\mathbb{Z})$ is the matrix of $(y_1, \ldots, y_n)$ written in a basis of M^*. ▷ Step 3 - Classical

Instead of a complexity analysis

The time complexity of HNF is heuristic $O(m^4)$ so the decrease of precision is $\widetilde{O}(m^4)$. Hence HNF on cyclotomic fields is faster than CHSP on arbitrary fields.

Conclusion

Reduction of number theory problems to (C)HSP

- factoring and DLP in abelian groups: HSP
- $\mathcal{O}_K^*$ and $\mathrm{Cl}(K)$ of fixed degree: HSP
- $\mathcal{O}_K^*$ and $\mathrm{Cl}(K)$ of arbitrary degree: CHSP
- $\mathcal{O}_K^*$ of cyclotomic fields: at least as fast as HSP