Regev’s LWE Reduction: the quantum part

Eamonn W. Postlethwaite

February 27, 2023

In [Reg09] an average case problem called “learning with errors” (LWE) is shown to reduce to two worst case problems over lattices.

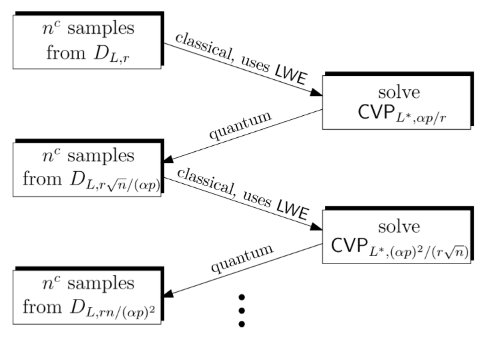
In [Reg09] an average case problem called “learning with errors” (LWE) is shown to reduce to two worst case problems over lattices.

- The worst case problems are called “[the] shortest independent vectors problem” (SIVP) and GapSVP,
- on input lattice L the reduction iterates two steps,
- the first step is entirely classical and uses an LWE oracle,
- the second step is quantum and uses the output of the first step,
- eventually the reduction outputs SIVP and GapSVP solutions on L.

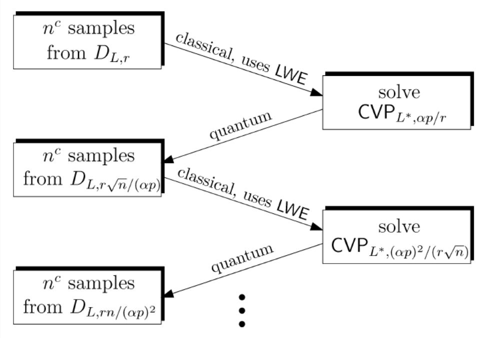
In [Reg09] an average case problem called “learning with errors” (LWE) is shown to reduce to two worst case problems over lattices.

- The worst case problems are called “[the] shortest independent vectors problem” (SIVP) and GapSVP,
- on input lattice L the reduction iterates two steps,
- the first step is entirely classical and uses an LWE oracle,
- the second step is quantum and uses the output of the first step,
- eventually the reduction outputs SIVP and GapSVP solutions on L.

The conclusion of the reduction is: if LWE is easy then SIVP and GapSVP are quantumly easy.

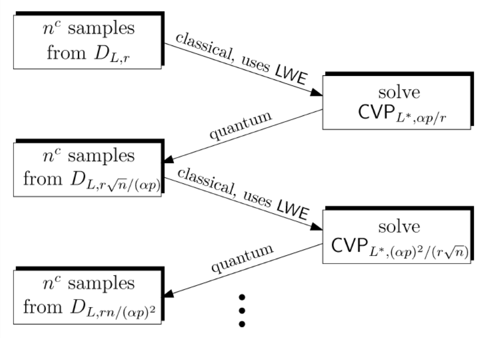


Each distribution on the lefthand side is over the SIVP and GapSVP challenge lattice L.



Each distribution on the lefthand side is over the SIVP and GapSVP challenge lattice L.

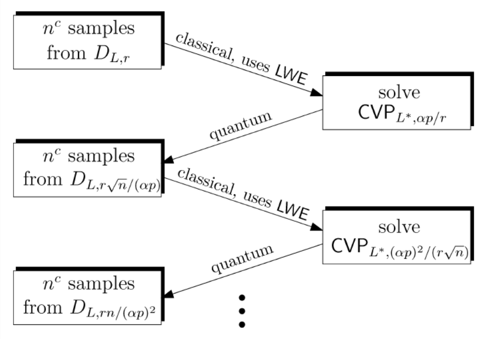
The topmost distribution is "wide" enough (r is large) that it can be efficiently sampled.



Each distribution on the lefthand side is over the SIVP and GapSVP challenge lattice L.

The topmost distribution is "wide" enough (r is large) that it can be efficiently sampled.

Each iteration returns the same number of samples from a "narrower" distribution. We have $\sqrt{n}/(\alpha p) < 1/2$.



Each distribution on the lefthand side is over the SIVP and GapSVP challenge lattice L.

The topmost distribution is “wide” enough (r is large) that it can be efficiently sampled.

Each iteration returns the same number of samples from a “narrower” distribution. We have $\sqrt{n}/(\alpha p) < 1/2$.

After enough iterations, the distribution is narrow enough to solve SIVP and GapSVP.

Think “a continuous Gaussian restricted to the points of a lattice”.

Definition (Discrete Gaussian distribution)
Let L be a lattice, $r > 0$ and $\rho_r : \mathbb{R}^n \to \mathbb{R},\ \mathbf{x} \mapsto \exp(-\pi\|\mathbf{x}/r\|^2)$, then

$$D_{L,r} : L \to \mathbb{R},\ \mathbf{x} \mapsto \rho_r(\mathbf{x})/\rho_r(L).$$

We use $\rho = \rho_1$.

Discrete Gaussians over lattices

Think "a continuous Gaussian restricted to the points of a lattice".

Definition (Discrete Gaussian distribution)
Let L be a lattice, $r > 0$ and $\rho_r \colon \mathbb{R}^n \to \mathbb{R},\ \mathsf{x} \mapsto \exp(-\pi\|\mathsf{x}/r\|^2)$, then

$$D_{L,r} \colon L \to \mathbb{R},\ \mathsf{x} \mapsto \rho_r(\mathsf{x})/\rho_r(L).$$

We use $\rho = \rho_1$.

Definition (Discrete Gaussian Sampling (DGS_r))
Given any basis B of L and $r > 0$ give an efficient algorithm that samples $D_{L,r}$.

LWE (just for fun...)

Think “learn (a secret from a linear system) with errors”.

Definition (Learning with Errors, search)
Let $n \in \mathbb{N}$, $p \geq 2$, $\mathbf{s} \in \mathbb{Z}_p^n$ and $\chi\colon \mathbb{Z}_p \to \mathbb{R}$ a pmf.

Define $A_{\mathbf{s},\chi}\colon \mathbb{Z}_p^n \times \mathbb{Z}_p \to \mathbb{R}$ as the pmf implied by $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + e)$ where $\mathbf{a} \leftarrow U(\mathbb{Z}_p^n)$ and $e \leftarrow \chi$.

Given oracle access to $A_{\mathbf{s},\chi}$ return $\mathbf{s}$.

SIVP and GapSVP

Think "many reasonably short independent vectors from L" and "tell me roughly how long the first minimum is (or isn't)".

Definition (SIVPγ)
Let $\gamma \geq 1$. Given a basis $\mathbf{B}$ of some lattice L return linearly independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n \in L$ with $\|\mathbf{x}_i\| \leq \gamma \cdot \lambda_n(L)$.

SIVP and GapSVP

Think "many reasonably short independent vectors from L" and "tell me roughly how long the first minimum is (or isn't)".

Definition (SIVPγ)
Let $\gamma \geq 1$. Given a basis $\mathbf{B}$ of some lattice L return linearly independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n \in L$ with $\|\mathbf{x}_i\| \leq \gamma \cdot \lambda_n(L)$.

Definition (GapSVP$_{\gamma,d}$)
Let $\gamma \geq 1$ and $d > 0$. Given a basis $\mathbf{B}$ of some lattice L and the promise that $\lambda_1(L) \leq d$ or $\lambda_1(L) > \gamma \cdot d$, return YES in the first case or NO in the second.

Solving SIVP via DGS (informally)

SIVP_γ: for lattice L assume a DGS oracle with $r > 0$

- small enough that $\mathbf{x} \leftarrow D_{L,r}$ has $\|\mathbf{x}\| \leq \gamma \cdot \lambda_n(L)$ with overwhelming probability,
- large enough that $\mathbf{x}$ behaves Gaussian enough (uses "smoothing parameter"),

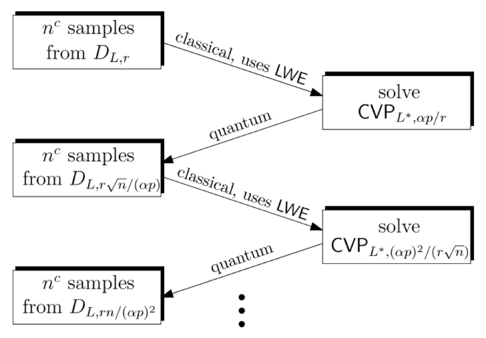
Solving SIVP via DGS (informally)

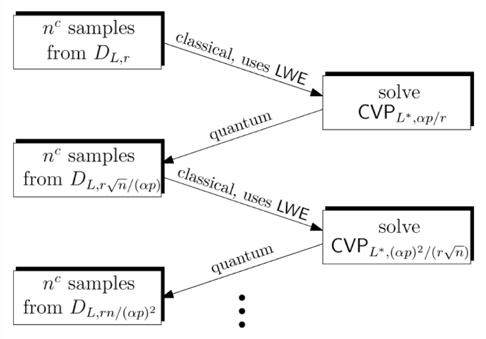
SIVP_γ: for lattice L assume a DGS oracle with $r > 0$

- small enough that $\mathbf{x} \leftarrow D_{L,r}$ has $\|\mathbf{x}\| \leq \gamma \cdot \lambda_n(L)$ with overwhelming probability,
- large enough that $\mathbf{x}$ behaves Gaussian enough (uses “smoothing parameter”),

then any n^2 i.i.d. samples $\{\mathbf{x}_i \leftarrow D_{L,r}\}_{i=1}^{n^2}$ contains a linearly independent set of size n with overwhelming probability [Reg09, Cor. 3.16].

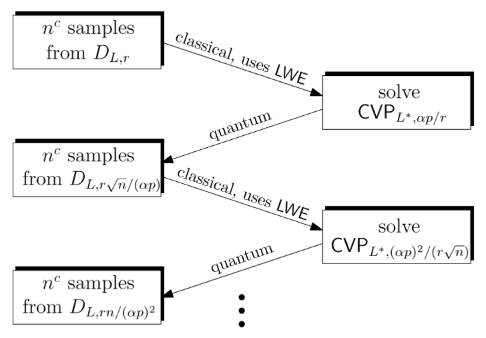
Given we are interested in the quantum arrow, we need to define this “CVP”.





Given we are interested in the quantum arrow, we need to define this "CVP".

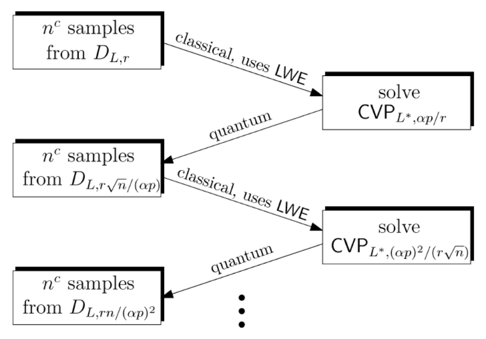
Then we show how to efficiently create a quantum state similar to one we wish to apply the QFT to.



Given we are interested in the quantum arrow, we need to define this "CVP".

Then we show how to efficiently create a quantum state similar to one we wish to apply the QFT to.

However the quantum state has an extra register and "uncomputing" this register is not reversible.



Given we are interested in the quantum arrow, we need to define this "CVP".

Then we show how to efficiently create a quantum state similar to one we wish to apply the QFT to.

However the quantum state has an extra register and "uncomputing" this register is not reversible.

The CVP oracle makes it reversible, so we uncompute the register and apply the QFT. Measuring the output state solves the next DGS instance.

Think "if I know how close a point is to the lattice, find the closest lattice vector to it."

Definition (CVP_d)
Let $d > 0$. Given a basis $\mathbf{B}$ of some lattice L and $\mathbf{t} \in \mathbb{R}^n$ such that $\mathrm{dist}(\mathbf{t}, L) \leq d$, find $\mathbf{x} \in L$ that minimises $\|\mathbf{x} - \mathbf{t}\|$.

Think "if I know how close a point is to the lattice, find the closest lattice vector to it."

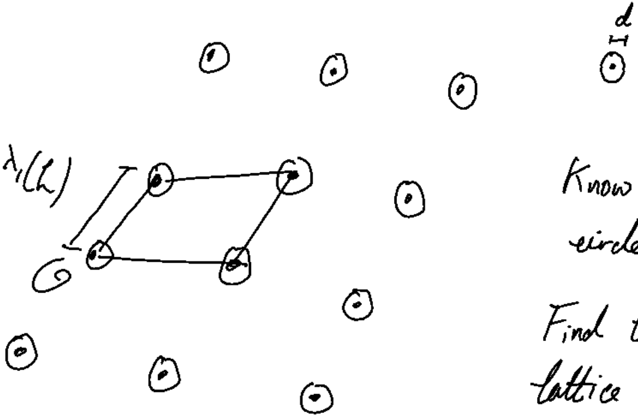
Definition (CVP_d)
Let $d > 0$. Given a basis $\mathbf{B}$ of some lattice L and $\mathbf{t} \in \mathbb{R}^n$ such that $\mathrm{dist}(\mathbf{t}, L) \leq d$, find $\mathbf{x} \in L$ that minimises $\|\mathbf{x} - \mathbf{t}\|$.

Throughout this definition coincides with BDD_γ for $\gamma = d/\lambda_1(L)$, as we always have $d < \lambda_1(L)/2$.

That is, there is a unique $\mathbf{x} \in L$ such that $\|\mathbf{x} - \mathbf{t}\| \leq d$.

$CVP_{L,d}$

$$d < \frac{\lambda_1(L)}{2}$$



Know t in some circle.

Find the unique lattice point in the same circle.

Prerequisites and Notes

All lattices will be full rank.

Definition (Lattice)
Given $\mathbf{B}$ in $\mathrm{GL}_n(\mathbb{R})$ the lattice generated by $\mathbf{B}$ is $L = \mathbf{B} \cdot \mathbb{Z}^n$.

Definition (Dual lattice)
Given a lattice L with basis $\mathbf{B}$, the dual lattice L^* has basis $\mathbf{B}^* = \mathbf{B}^{-t}$ and equals $\{\mathbf{x} \in \mathbb{R}^n \colon \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}$.

Definition (Minima)
For $i \in \{1, \ldots, n\}$, $\lambda_i(L)$ is the minimum length such that $\bar{B}_n(\lambda_i(L)) \cap L$ contains i linearly independent vectors.

Prerequisites and Notes

I will *not* be keeping track of normalisation constants for quantum states.

Definition
Given basis $\mathbf{B}$ of lattice L, $\mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot [0, 1)^n$.

Lemma (Babai [Bab86])
Given a basis $\mathbf{B}$ *of lattice* L *and* $\mathbf{t} \in \mathbb{R}^n$*, one can efficiently find* $\mathbf{x} \in L$ *with* $\|\mathbf{x} - \mathbf{t}\| \leq 2^{n/2} \cdot \mathrm{dist}(\mathbf{t}, L)$.

Lemma (Efficient creation of distribution [GR02])
Given an efficiently integrable pdf $p \colon \mathbb{R} \to \mathbb{R}$ *let* $\{p_i\}_i$ *be a pmf formed by discretisation. One can efficiently create the state*

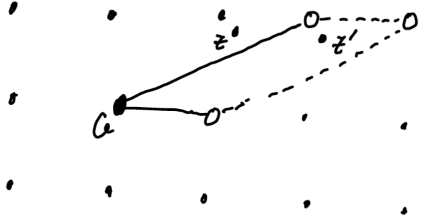
$$\sum_i \sqrt{p_i} \left| i \right\rangle .$$

$L = \mathbb{Z}^2$

- $B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

- $\bigcup_{x \in L} (x + \mathcal{P}(B)) = \mathbb{R}^2$

- $x, y \in L, \quad x + \mathcal{P}(B) = y + \mathcal{P}(B) \Leftrightarrow x = y$



$z' = z \bmod \mathcal{P}(B)$

$dist(z, L) = dist(z', L)$

The main theorem

Theorem ([Reg09, Lem. 3.14])
Given

- *any basis* $\mathbf{B}$ *of any lattice* L,
- *some* $0 < d < \lambda_1(L^*)/2$,
- *a* $CVP_{L^*,d}$ *oracle,*

there exists an efficient quantum algorithm that samples $D_{L,\sqrt{n}/(\sqrt{2}d)}$.

The main theorem

Theorem ([Reg09, Lem. 3.14])
Given

- *any basis* $\mathbf{B}$ *of any lattice* L,
- *some* $0 < d < \lambda_1(L^*)/2$,
- *a* $\mathrm{CVP}_{L^*,d}$ *oracle,*

there exists an efficient quantum algorithm that samples $D_{L,\sqrt{n}/(\sqrt{2}d)}$.

To clean up notation, if $d = c\sqrt{n}$ then scale $L \to c \cdot L$ and $L^* \to (1/c) \cdot L$.

The main theorem

Theorem ([Reg09, Lem. 3.14])
Given

- *any basis* B *of any lattice* L,
- *some* $0 < \sqrt{n} < \lambda_1(L^*)/2$,
- *a* $CVP_{L^*,\sqrt{n}}$ *oracle*,

there exists an efficient quantum algorithm that samples $D_{L,1/\sqrt{2}}$.

To clean up notation, if $d = c\sqrt{n}$ then scale $L \to c \cdot L$ and $L^* \to (1/c) \cdot L$.

Two technical lemmata (I)

Think “for a large enough width, I can create a discrete Gaussian quantum superposition over an integer lattice”.

Lemma ([Reg09, Lem. 3.12])
Given a basis $\mathbf{B}$ *of lattice* $L \subset \mathbb{Z}^n$ *and a width* $r > 2^{2n}\lambda_n(L)$*, there is an efficient quantum algorithm to create**

$$\sum_{\mathbf{x} \in L} \sqrt{\rho_r(\mathbf{x})} \, |\mathbf{x}\rangle = \sum_{\mathbf{x} \in L} \rho_{\sqrt{2}r}(\mathbf{x}) \, |\mathbf{x}\rangle .$$

Two technical lemmata (I)

Think “for a large enough width, I can create a discrete Gaussian quantum superposition over an integer lattice”.

Lemma ([Reg09, Lem. 3.12])
Given a basis $\mathbf{B}$ *of lattice* $L \subset \mathbb{Z}^n$ *and a width* $r > 2^{2n}\lambda_n(L)$*, there is an efficient quantum algorithm to create**

$$\sum_{\mathbf{x}\in L} \sqrt{\rho_r(\mathbf{x})}\,|\mathbf{x}\rangle = \sum_{\mathbf{x}\in L} \rho_{\sqrt{2}r}(\mathbf{x})\,|\mathbf{x}\rangle.$$

Intution: use [GR02] to first create*

$$\sum_{\mathbf{x}\in\mathbb{Z}^n} \rho_{\sqrt{2}r}(\mathbf{x})\,|\mathbf{x}\rangle,$$

then compute $\mathbf{x} \bmod \mathcal{P}(\mathrm{LLL}(\mathbf{B}))$ in another register and measure.

Two technical lemmata (II)

Think, “most of the weight of ρ is on points of length less than $\sqrt{n}$”.

Lemma ([Reg09, Lem. 3.13])
Let R be a positive integer and B *as basis for lattice L with $\lambda_1(L) > 2\sqrt{n}$. The following two states are the same*,*

$$|\nu_1\rangle = \sum_{\mathsf{x} \in L/R, \|\mathsf{x}\| < \sqrt{n}} \rho(\mathsf{x}) \, |\mathsf{x} \bmod \mathcal{P}(\mathsf{B})\rangle \qquad \text{and}$$

$$|\nu_2\rangle = \sum_{\mathsf{x} \in L/R} \rho(\mathsf{x}) \, |\mathsf{x} \bmod \mathcal{P}(\mathsf{B})\rangle = \sum_{\mathsf{x} \in L/R \cap \mathcal{P}(\mathsf{B})} \sum_{\mathsf{y} \in L} \rho(\mathsf{x} - \mathsf{y}) \, |\mathsf{x}\rangle.$$

Two technical lemmata (II)

Think, “most of the weight of ρ is on points of length less than $\sqrt{n}$”.

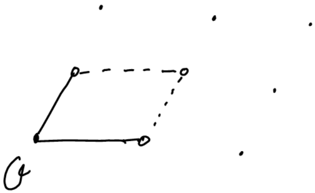
Lemma ([Reg09, Lem. 3.13])
Let R be a positive integer and $\mathbf{B}$ *as basis for lattice L with $\lambda_1(L) > 2\sqrt{n}$. The following two states are the same*,*

$$|\nu_1\rangle = \sum_{\mathbf{x}\in L/R, \|\mathbf{x}\|<\sqrt{n}} \rho(\mathbf{x})\, |\mathbf{x} \bmod \mathcal{P}(\mathbf{B})\rangle \qquad \text{and}$$

$$|\nu_2\rangle = \sum_{\mathbf{x}\in L/R} \rho(\mathbf{x})\, |\mathbf{x} \bmod \mathcal{P}(\mathbf{B})\rangle = \sum_{\mathbf{x}\in L/R\cap\mathcal{P}(\mathbf{B})} \sum_{\mathbf{y}\in L} \rho(\mathbf{x}-\mathbf{y})\, |\mathbf{x}\rangle .$$

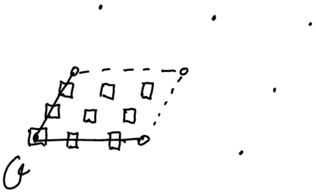
Intuition: that $\lambda_1(L) > 2\sqrt{n}$ means each ket in the sum $|\nu_1\rangle$ takes a unique value, then tail bounds for Gaussian weights.

Two technical lemmata (II)



$n = 2$ lattice $\mathcal{L}$ with $\mathcal{P}(B)$ drawn.

If $R = 1$, $\mathcal{L}/R = \mathcal{L}$, then $\forall x \in \mathcal{L}$ $x \bmod \mathcal{P}(B) = 0$



If $R = 3$, then for $x \in \mathcal{L}/R$ $x \bmod \mathcal{P}(B)$ is one of the $\square$s.

Sketch of main theorem

Theorem ([Reg09, Lem. 3.14])
Given

- *any basis* B *of any lattice* L,
- *some* $0 < \sqrt{n} < \lambda_1(L^*)/2$,
- *a* $\mathrm{CVP}_{L^*,\sqrt{n}}$ *oracle*,

Sketch of main theorem

Step 1: set integer $R \geq 2^{3n} \cdot \lambda_n(L^*)$.

Step 2: create* $\displaystyle\sum_{\mathbf{x} \in L^*/R \cap \mathcal{P}(\mathbf{B}^*)} \sum_{\mathbf{y} \in L^*} \rho(\mathbf{x} - \mathbf{y}) \left|\mathbf{x}\right\rangle$.

Step 3: perform the quantum Fourier transform on it.

Step 4: show the output state, after applying Babai's algorithm, is correctly distributed.

Sketch of main theorem

Step 1: set integer $R \geq 2^{3n} \cdot \lambda_n(L^*)$. (Allows us to scale L^* down enough to use (I).)

Step 2: create* $\displaystyle\sum_{\mathbf{x} \in L^*/R \cap \mathcal{P}(\mathbf{B}^*)} \sum_{\mathbf{y} \in L^*} \rho(\mathbf{x} - \mathbf{y}) \, |\mathbf{x}\rangle.$

Step 3: perform the quantum Fourier transform on it.

Step 4: show the output state, after applying Babai's algorithm, is correctly distributed.

Sketch of main theorem

Step 1: set integer $R \geq 2^{3n} \cdot \lambda_n(L^*)$. (Allows us to scale L^* down enough to use (I).)

Step 2: create* $\sum_{\mathbf{x} \in L^*/R \cap \mathcal{P}(\mathbf{B}^*)} \sum_{\mathbf{y} \in L^*} \rho(\mathbf{x} - \mathbf{y}) |\mathbf{x}\rangle$. (This is the rhs of $|\nu_2\rangle$ with L^* in (II), so create $|\nu_1\rangle$ via (I).)

Step 3: perform the quantum Fourier transform on it.

Step 4: show the output state, after applying Babai's algorithm, is correctly distributed.

Sketch of main theorem

Step 1: set integer $R \geq 2^{3n} \cdot \lambda_n(L^*)$. (Allows us to scale L^* down enough to use (I).)

Step 2: create* $\sum_{\mathbf{x} \in L^*/R \cap \mathcal{P}(\mathbf{B}^*)} \sum_{\mathbf{y} \in L^*} \rho(\mathbf{x} - \mathbf{y}) \left|\mathbf{x}\right\rangle$. (This is the rhs of $|\nu_2\rangle$ with L^* in (II), so create $|\nu_1\rangle$ via (I).)

Step 3: perform the quantum Fourier transform on it. (Translate to a finite abelian group setting and argue via characters.)

Step 4: show the output state, after applying Babai's algorithm, is correctly distributed.

Sketch of main theorem

Step 1: set integer $R \geq 2^{3n} \cdot \lambda_n(L^*)$. (Allows us to scale L^* down enough to use (I).)

Step 2: create* $\sum_{\mathbf{x} \in L^*/R \cap \mathcal{P}(\mathbf{B}^*)} \sum_{\mathbf{y} \in L^*} \rho(\mathbf{x} - \mathbf{y}) |\mathbf{x}\rangle$. (This is the rhs of $|\nu_2\rangle$ with L^* in (II), so create $|\nu_1\rangle$ via (I).)

Step 3: perform the quantum Fourier transform on it. (Translate to a finite abelian group setting and argue via characters.)

Step 4: show the output state, after applying Babai's algorithm, is correctly distributed.

Step 2 requires the CVP oracle. Step 3 is the only quantum bit.

Step 2

We want to create

$$|\nu_1\rangle = \sum_{\mathbf{x}\in L^*/R, \|\mathbf{x}\|<\sqrt{n}} \rho(\mathbf{x}) \, |\mathbf{x} \bmod \mathcal{P}(\mathbf{B}^*)\rangle.$$

We can use (I) with $r = 1/\sqrt{2}$ to create

$$\sum_{\mathbf{x}\in L^*/R, \|\mathbf{x}\|<\sqrt{n}} \rho(\mathbf{x}) \, |\mathbf{x}\rangle.$$

Then we can compute into another register the reduction of $\mathbf{x}$ modulo our $\mathcal{P}(\mathbf{B}^*)$

$$\sum_{\mathbf{x}\in L^*/R, \|\mathbf{x}\|<\sqrt{n}} \rho(\mathbf{x}) \, |\mathbf{x}, \mathbf{x} \bmod \mathcal{P}(\mathbf{B}^*)\rangle.$$

Step 2, problem and solution

The problem is that we cannot uncompute (forget, set to 0, etc...) the first register, as all quantum operations must be unitary $\leftrightarrow$ reversible.

Step 2, problem and solution

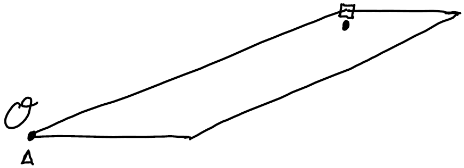
The problem is that we cannot uncompute (forget, set to 0, etc...) the first register, as all quantum operations must be unitary $\leftrightarrow$ reversible.

We have set our parameters such that the $\mathrm{CVP}_{L^*,\sqrt{n}}$ oracle allows us to make this reversible.

Some $\mathcal{P}(B^*)$ drawn. Let

$\bullet = x \bmod \mathcal{P}(B^*)$

$\square = CVP_{\mathcal{L}^*, \sqrt{n}}(x \bmod \mathcal{P}(B^*))$



- $dist(x \bmod \mathcal{P}(B^*), \mathcal{L}^*) < \sqrt{n}$
- $\lambda_1(\mathcal{L}^*) > 2\sqrt{n}$
- $CVP_{\mathcal{L}^*, \sqrt{n}}$ oracle

$\Rightarrow$ $\Delta = \bullet - \square$ is x recovered from $x \bmod \mathcal{P}(B^*)$

Step 3

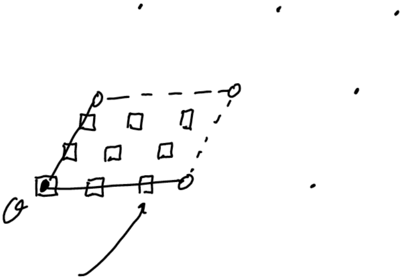
We assume that from Step 2 we have*

$$\sum_{\mathbf{x} \in L^*/R \cap \mathcal{P}(\mathbf{B}^*)} \sum_{\mathbf{y} \in L^*} \rho(\mathbf{x} - \mathbf{y}) \, |\mathbf{x}\rangle.$$

Thinking of $L^*/R \cap \mathcal{P}(\mathbf{B}^*)$ as $\mathbb{Z}_R^n$ this state is equal to

$$\sum_{\mathbf{s} \in \mathbb{Z}_R^n} \rho(\mathbf{B}^*\mathbf{s}/R - L^*) \, |\mathbf{s}\rangle.$$

Some lattice L^* with $P(B^*)$ and $R=3$



$s = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$

$\square \quad x \in \frac{L^*}{R} \cap P(B^*)$

can label with

$s \in \mathbb{Z}_R^n$

$\frac{B^* s}{3} \longleftrightarrow x$

Step 3, quantum Fourier transform

Let

$$f : \mathbb{Z}_R^n \to \mathbb{C},\ \mathbf{s} \mapsto \rho(\mathbf{B}^* \mathbf{s}/R - L^*)$$

and $\mathbf{t} \in \widehat{\mathbb{Z}_R^n}$ be a character.

We can associate $\mathbf{t}$ with $(t_1, \ldots, t_n) \in \mathbb{Z}_R^n$ such that

$$\mathbf{t}(\mathbf{s}) = \prod_{j=1}^{n} \exp(2\pi i\, s_j t_j / R) = \exp\left(2\pi i\, \mathbf{s} \cdot \mathbf{t}/R\right).$$

Step 3, quantum Fourier transform

Let

$$f : \mathbb{Z}_R^n \to \mathbb{C},\ \mathbf{s} \mapsto \rho(\mathbf{B}^* \mathbf{s}/R - L^*)$$

and $\mathbf{t} \in \widehat{\mathbb{Z}_R^n}$ be a character.

We can associate $\mathbf{t}$ with $(t_1, \ldots, t_n) \in \mathbb{Z}_R^n$ such that

$$\mathbf{t}(\mathbf{s}) = \prod_{j=1}^{n} \exp(2\pi i\, s_j t_j / R) = \exp\left(2\pi i\, \mathbf{s} \cdot \mathbf{t}/R\right).$$

Finally, $\hat{f}(\mathbf{t}) = \sum_{\mathbf{s} \in \mathbb{Z}_R^n} f(s)\bar{\mathbf{t}}(\mathbf{s}) = \sum_{\mathbf{s} \in \mathbb{Z}_R^n} \rho(\mathbf{B}^* \mathbf{s}/R - L^*) \exp(-2\pi i\, \mathbf{s} \cdot \mathbf{t}/R)$.

Step 3, quantum Fourier transform

This says that $|\mathbf{t}\rangle$ in the quantum Fourier transform of

$$\sum_{\mathbf{s}\in\mathbb{Z}_R^n} \rho(\mathbf{B}^*\mathbf{s}/R - L^*)\,|\mathbf{s}\rangle.$$

has amplitude

$$\alpha_{\mathbf{t}} = \sum_{\mathbf{s}\in\mathbb{Z}_R^n} \rho(\mathbf{B}^*\mathbf{s}/R - L^*)\exp(-2\pi i\,\mathbf{s}\cdot\mathbf{t}/R)$$

Step 3, quantum Fourier transform

This says that $|\mathsf{t}\rangle$ in the quantum Fourier transform of

$$\sum_{\mathsf{s}\in\mathbb{Z}_R^n} \rho(\mathsf{B}^*\mathsf{s}/R - L^*)\,|\mathsf{s}\rangle.$$

has amplitude

$$\alpha_{\mathsf{t}} = \sum_{\mathsf{s}\in\mathbb{Z}_R^n} \rho(\mathsf{B}^*\mathsf{s}/R - L^*)\exp(-2\pi i\,\mathsf{s}\cdot\mathsf{t}/R)$$

A long chain of equalities (involving Poisson summation) tells us $\sum_{\mathsf{t}} \alpha_{\mathsf{t}}\,|\mathsf{t}\rangle$ is equal to

$$\sum_{\mathsf{x}\in L\cap\mathcal{P}(R\mathsf{B})}\ \sum_{\mathsf{y}\in RL} \rho(\mathsf{x}-\mathsf{y})\,|\mathsf{x}\rangle.$$

Step 4

We can apply (II) "in reverse" to show that $|\mathbf{t}\rangle$ has amplitude

$$\sum_{\mathbf{x} \in L, \|\mathbf{x}\| < \sqrt{n}} \rho(\mathbf{x}) \, |\mathbf{x} \bmod \mathcal{P}(R\mathbf{B})\rangle.$$

Measuring this state gives us some $\mathbf{x} \bmod \mathcal{P}(R\mathbf{B})$ with probability (proportional to) $\rho(\mathbf{x})^2 = \rho_{1/\sqrt{2}}(\mathbf{x})$ for some $\mathbf{x} \in L$ with $\|\mathbf{x}\| < \sqrt{n}$.

Step 4

We can apply (II) "in reverse" to show that $|\mathbf{t}\rangle$ has amplitude

$$\sum_{\mathbf{x}\in L, \|\mathbf{x}\| < \sqrt{n}} \rho(\mathbf{x}) \, |\mathbf{x} \bmod \mathcal{P}(R\mathbf{B})\rangle.$$

Measuring this state gives us some $\mathbf{x} \bmod \mathcal{P}(R\mathbf{B})$ with probability (proportional to) $\rho(\mathbf{x})^2 = \rho_{1/\sqrt{2}}(\mathbf{x})$ for some $\mathbf{x} \in L$ with $\|\mathbf{x}\| < \sqrt{n}$.

It remains to note that

- all* of the mass of ρ is below $\sqrt{n}$, and
- since $\mathrm{dist}(\mathbf{x} \bmod \mathcal{P}(R\mathbf{B}), L) < \sqrt{n}$ and $\lambda_1(RL) \geq 2^{3n}$ we can recover $\mathbf{x}$ with Babai's algorithm.

Discussion

- has been partially [Pei09] and then entirely [BLP+13] dequantised,
- can our thinking be “reversed” and this argument used to (quantumly) sample from lattices,
- a paper of Eldar and Shor [ES17] also considers quantum sampling from lattices via a similar approach – they construct a particular “lattice” DFT for lattices with basis in “systematic normal form”.

L. Babai.
On Lovász' lattice reduction and the nearest lattice point problem.
Combinatorica, 6(1):1–13, 1986.

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé.
Classical hardness of learning with errors.
In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '13, page 575–584, New York, NY, USA, 2013. Association for Computing Machinery.

Lior Eldar and Peter Shor.
A discrete fourier transform on lattices with quantum applications, 2017.

Lov Grover and Terry Rudolph.

Creating superpositions that correspond to efficiently integrable probability distributions, 2002.

Chris Peikert.
Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract.
In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 333–342, New York, NY, USA, 2009. Association for Computing Machinery.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
J. ACM, 56(6), Sep 2009.