

Attempts to Quantumly Solve Standard Lattice Problems: Quantum Reduction from SVP to $S|LWE\rangle$ and Beyond

Zihan Hu, Yaxin Tu
(Authors of this note)

Yilei Chen
(Dear advisor)

Qipeng Liu
(Dear collaborator)

December 20, 2022

Contents

1	Introduction	1
2	Quantum reduction from SVP to $S LWE\rangle$	1
2.1	Summary of Regev's reduction [Reg09]	1
2.2	Modifying Regev's reduction	2
3	Extracting secrets from $LWE\rangle$ state	4
3.1	Measuring the overlap of $ \psi_{\langle s, a \rangle, y}\rangle$ and uniform to approximate $\ \mathbf{x}'\ $	4
3.2	The distribution of \mathbf{y}	4
3.3	Use \mathbf{y} when measuring $ \psi_{\langle s, a \rangle, y}\rangle$	6
4	Other possible methods	7
4.1	Bypassing $ LWE\rangle$	7
A	Appendix	8
A.1	An extension of Banaszczyk's Gaussian tail bounds over lattices	8
A.2	Smoothing of Gaussian with a phase	11
A.3	Linear combination of continuous Gaussian with a phase	12

1 Introduction

In this note, we summarize our partial results on solving standard lattice problems, e.g., the shortest vector problem (SVP).

Solving SVP over lattices has been a target for designing efficient quantum algorithms for decades. Regev [Reg09] shows given a polynomial time algorithm that solves $\text{LWE}_{n,m,q,\mathcal{D}_{\text{noise}}}$ where $\mathcal{D}_{\text{noise}}$ is Gaussian and m can be any polynomial, one can construct a quantum algorithm that solves worst-case approximate SVP.

Here let us consider the following quantum variant of the LWE problem called solving LWE given LWE-like states (S|LWE).

Definition 1 (Solving LWE given LWE-like quantum states (S|LWE)). *Let n, m, q be positive integers. Let f be a function from \mathbb{Z}_q to \mathbb{R} . Let $u \in \mathbb{Z}_q^n$ be a secret vector. The problem of solving LWE given LWE-like states $\text{S|LWE}\rangle_{n,m,q,f}$ asks to find u given access to an oracle that outputs $a_i, \sum_{e_i \in \mathbb{Z}_q} f(e_i) |a_i \cdot u + e_i \pmod{q}\rangle$ on its i^{th} query, for $i = 1, \dots, m$. Here each a_i is a uniformly random vector in \mathbb{Z}_q^n .*

$\text{S|LWE}\rangle_{n,m,q,\sqrt{D_{\text{noise}}}}$ is easier to solve than $\text{LWE}_{n,m,q,D_{\text{noise}}}$, because we can get (classical) LWE samples by measuring $|\text{LWE}\rangle$ in computational basis. Recent work [CLZ21] shows when the noise amplitude f is of a special kind, we can solve $\text{S|LWE}\rangle$ in quantum polynomial time.

Theorem 2 ([CLZ21]). *When the noise distribution f is chosen such that \hat{f} is non-negligible over \mathbb{Z}_q , then we can solve $\text{S|LWE}\rangle_{n,m,q,f}$ in quantum polynomial time.*

Given the ‘feasibility’ of $\text{S|LWE}\rangle$, one plausible roadmap towards solving SVP is first modify Regev’s reduction (from SVP to LWE) to a reduction from SVP to $\text{S|LWE}\rangle$, and then solve the $\text{S|LWE}\rangle$ problem. The key point is that the noise amplitude f in $\text{S|LWE}\rangle$ should on one hand be ‘strong’ enough so that the $\text{S|LWE}\rangle$ oracle can solve SVP problem, but on the other hand be ‘weak’ enough so that the $\text{S|LWE}\rangle$ problem is solvable by polynomial quantum algorithms.

2 Quantum reduction from SVP to $\text{S|LWE}\rangle$

In this section, we’ll show how to obtain a quantum reduction from SVP to $\text{S|LWE}\rangle$, by modifying Regev’s reduction from SVP to LWE.

2.1 Summary of Regev’s reduction [Reg09]

Let’s start by recalling the details of Regev’s reduction. SVP (or other standard lattice problem) can be reduced to sampling from the discrete Gaussian distribution ($D_{L,r}$) of a nontrivial width r over the lattice L . With the help of an LWE solver, one can construct a procedure sampling from $D_{L,r}$ given samples from $D_{L,r \cdot c}$ with $c > 1$, and hence can start with samples from extremely wide $D_{L,R}$ (which can be obtained through, say, LLL-algorithm) and end up with samples from $D_{L,r}$ with a nontrivial (say, polynomial) width r . The precise procedure contains two subroutines:

Step 1 (Classical, uses LWE) Given an instance of $\text{CVP}_{L^*, \alpha q / (\sqrt{2}r)}$, using $\text{poly}(n)$ samples from $D_{L,r}$ to create LWE samples with Gaussian noise with width $\leq \alpha q$, and then solve it with an LWE solver which in turn solves the $\text{CVP}_{L^*, \alpha q / (\sqrt{2}r)}$ problem:

Lemma 3 ([Reg09]). *Suppose $m \in \text{poly}(n)$, q be an integer, $\alpha \in (0, 1)$ be a real number and $r > \sqrt{2}q\eta_\epsilon(L)$ satisfying some smoothing condition with $\epsilon \in \text{negl}(n)$. There exists an efficient (classical) algorithm that, given an oracle that solves $\text{LWE}_{n,m,q,q\Psi_\alpha}$ and $\text{poly}(n, m)$ samples from $D_{L,r}$, solves $\text{CVP}_{L^*, \alpha q / (\sqrt{2}r)}$, where Ψ_α denotes the periodic Gaussian distribution and $q\Psi_\alpha$ stands for scaling it by q .*

Step 2 (Quantum) Using a $\text{CVP}_{L^*, \alpha q / (\sqrt{2}r)}$ solver to generate $\text{poly}(n)$ discrete Gaussian states $|D_{L,r\sqrt{n}/(\alpha q)}\rangle = \sum_{\mathbf{v} \in L} \sqrt{\rho_{r\sqrt{n}/(\alpha q)}(\mathbf{v})} |\mathbf{v}\rangle$ and measure them to get $\text{poly}(n)$ classical samples from $D_{L,r\sqrt{n}/\alpha q}$:

Lemma 4 ([Reg09]). *There exists an efficient quantum algorithm that, given any n -dimensional lattice L , a number $d < \lambda_1(L^*)/2$, and an oracle that solves $\text{CVP}_{L^*, d}$, outputs $|D_{L,\sqrt{n}/(\sqrt{2}d)}\rangle$.*

These two subroutines allow us to transform the distribution $D_{L,r}$ to a narrower distribution $D_{L,r\sqrt{n}/(\alpha q)}$, and hence solve the discrete Gaussian sampling problem whenever $\alpha q / \sqrt{n} > 1$.

2.2 Modifying Regev's reduction

Notice that the quantum part of the iterative algorithm actually produces discrete Gaussian states instead of just classical samples. This gives us hope to construct a procedure sampling $|D_{L,r}\rangle$ states, given $|D_{L,r\cdot c}\rangle$ ($c > 1$) states and an $\text{S|LWE}\rangle$ solver. The procedure is as follows:

Step 1 (Uses $\text{S|LWE}\rangle$) Given an instance of $\text{CVP}_{L^*, \alpha q / r}$, using $\text{poly}(n)$ discrete Gaussian states $|D_{L,r}\rangle$ to create an $\text{S|LWE}\rangle_{n,m,q,f}$ instance with certain f , and then solve it with an $\text{S|LWE}\rangle_{n,m,q,f}$ solver which in turn solves the $\text{CVP}_{L^*, \alpha q / r}$ problem;

Step 2 (Same as the quantum step in Regev's reduction) Using a $\text{CVP}_{L^*, \alpha q / (\sqrt{2}r)}$ solver to generate $\text{poly}(n)$ discrete Gaussian states $|D_{L,r\sqrt{n}/(\alpha q)}\rangle = \sum_{\mathbf{v} \in L} \sqrt{\rho_{r\sqrt{n}/(\alpha q)}(\mathbf{v})} |\mathbf{v}\rangle$;

Step 3 (Additional) Create arbitrarily polynomially many *quantum* states $|D_{L,r'}\rangle$ from $\text{poly}(n)$ $|D_{L,r\sqrt{n}/(\alpha q)}\rangle$ states, where $r\sqrt{n}/\alpha q < r' < r$.

Step 3 appears in case the $\text{S|LWE}\rangle$ solver in step 1 need to consume $|D_{L,r}\rangle$ states. Step 3 can be done in multiple ways, e.g., slightly modifying the GPV discrete Gaussian sampler [GPV08] to sample $|D_{L,r'}\rangle$ states with $r' = r \cdot (n\omega(\sqrt{\log n})/(\alpha q))$. In this case we should demand $\alpha q > n\omega(\sqrt{\log n})$.

We are left with step 1 to close the reduction. In the sequel, we focus on doing step 1 and see the $\text{S|LWE}\rangle$ oracle we require.

Let \mathbf{x} denote a $\text{CVP}_{L^*, \alpha q / r}$ instance. Write $\mathbf{x} = \kappa_{L^*}(\mathbf{x}) + \mathbf{x}'$, where $\kappa_{L^*}(\mathbf{x})$ is the closest L^* vector to \mathbf{x} , then it is guaranteed that $\|\mathbf{x}'\| \leq \alpha q / r$.

According to Regev's reduction, $\langle \mathbf{x}, \mathbf{v} \rangle + e \pmod{p} = \langle \kappa_{L^*}(\mathbf{x}), \mathbf{v} \rangle + (\langle \mathbf{x}', \mathbf{v} \rangle + e) \pmod{p}$ is an LWE instance where \mathbf{v} is a $D_{L,r}$ sample, and e is sampled from Gaussian distribution to “smooth” the discrete Gaussian $\langle \mathbf{x}', \mathbf{v} \rangle$.

Here we follow the same idea to prepare $|\text{LWE}\rangle$ state through the following steps, using the discrete Gaussian state to replace the discrete Gaussian distribution over the lattice and a pure state with Gaussian amplitudes to replace the Gaussian error. For simplicity, let's ignore the normalization factors.

1. Prepare the initial state

$$\sum_{\mathbf{v} \in L} \rho_{r\sqrt{2}}(\mathbf{v}) |\mathbf{v}\rangle \otimes \sum_{e \in \mathbb{R}} \rho_{\sqrt{2}\sigma}(e) |e \bmod q\rangle$$

($\sum_{e \in \mathbb{R}}$ is not well-defined, we *will* build a state with enough precision to replace it.)

2. Measure $L^{-1}\mathbf{v} \bmod q$ to get an outcome \mathbf{a} and a result state

$$\sum_{\mathbf{v} \in qL + L\mathbf{a}} \rho_{r\sqrt{2}}(\mathbf{v}) |\mathbf{v}\rangle \otimes \sum_{e \in \mathbb{R}} \rho_{\sqrt{2}\sigma}(e) |e \bmod q\rangle$$

3. Apply a unitary to add the inner product $\langle \mathbf{x}, \mathbf{v} \rangle \bmod q$ to the second register we get

$$\sum_{\mathbf{v} \in qL + L\mathbf{a}} \rho_{r\sqrt{2}}(\mathbf{v}) |\mathbf{v}\rangle \otimes \sum_{e \in \mathbb{R}} \rho_{\sqrt{2}\sigma}(e) |\langle \mathbf{s}, \mathbf{a} \rangle + \langle \mathbf{x}', \mathbf{v} \rangle + e \bmod q\rangle$$

where $L^*\mathbf{s} = \kappa_L^*(\mathbf{x}) \pmod{p}$.

4. Apply QFT_R to the first register where $R > r\sqrt{n}$ is an integer:

$$\sum_{\mathbf{y} \in \mathbb{Z}_R^n} \sum_{\mathbf{v} \in qL + L\mathbf{a}} \rho_{r\sqrt{2}}(\mathbf{v}) \cdot \omega_R^{\langle \mathbf{v}, \mathbf{y} \rangle} |\mathbf{y}\rangle \otimes \sum_{e \in \mathbb{R}} \rho_{\sqrt{2}\sigma}(e) |\langle \mathbf{s}, \mathbf{a} \rangle + \langle \mathbf{x}', \mathbf{v} \rangle + e \bmod q\rangle, \quad (1)$$

5. Measure the first register to get an outcome \mathbf{y} and a result state

$$\sum_{\mathbf{v} \in qL + L\mathbf{a}} \sum_{e \in \mathbb{R}} \rho_{r\sqrt{2}}(\mathbf{v}) \rho_{\sqrt{2}\sigma}(e) \cdot \omega_R^{\langle \mathbf{v}, \mathbf{y} \rangle} |\langle \mathbf{s}, \mathbf{a} \rangle + \langle \mathbf{x}', \mathbf{v} \rangle + e \bmod q\rangle. \quad (2)$$

According to [theorem 12](#), this state is close to:

$$|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle := \sum_{u' \in \mathbb{R}} \rho_{\sqrt{2}\sqrt{r^2\|\mathbf{x}'\|^2 + \sigma^2}}(u') \cdot e^{2\pi i \cdot u' \cdot \theta} |\langle \mathbf{s}, \mathbf{a} \rangle + u' \bmod q\rangle, \quad (3)$$

an LWE-like state whose error distribution is Gaussian distribution with a phase, where $\theta := \frac{r^2\langle \mathbf{x}', \mathbf{y}'/R \rangle}{r^2\|\mathbf{x}'\|^2 + \sigma^2}$, $\mathbf{y}'/R := \mathbf{y}/R - \kappa_{(qL)^*}(\mathbf{y}/R)$.

Hence, if one can solve \mathbf{s} from $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle$, an $|\text{LWE}\rangle$ with error distribution being Gaussian distribution with a phase, then one can solve the $\text{CVP}_{L^*, \alpha q/r}$ problem.

One caveat is this $\text{S}|\text{LWE}\rangle_{n,m,q,f}$ problem has its amplitude function $f(u) = \rho_{\sqrt{2}\sqrt{r^2\|\mathbf{x}'\|^2 + \sigma^2}}(u) \cdot e^{2\pi i \cdot u \cdot \theta}$ which depends on \mathbf{x}' and known \mathbf{y} .

To eventually solve the CVP problem for \mathbf{x} , it suffices to extract either the center $\langle \mathbf{s}, \mathbf{a} \rangle$, or $\|\mathbf{x}'\|$, or the direction of \mathbf{x}' from the state 3. In the following sections, we will describe our attempts and partial results.

Remark 5. *If there is no phase (i.e. $\mathbf{y} = \mathbf{0}$), this state can be written as*

$$\sum_{e' \in \mathbb{R}} \rho_{\sqrt{2}\sqrt{r^2\|\mathbf{x}'\|^2 + \sigma^2}}(e') |\langle \mathbf{s}, \mathbf{a} \rangle + e' \bmod q\rangle, \quad (4)$$

an $|\text{LWE}\rangle$ with Gaussian error distribution. It is the phase that makes our $|\text{LWE}\rangle$ nonstandard.

3 Extracting secrets from $|\text{LWE}\rangle$ state

From now on our targets become extracting either the center $\langle \mathbf{s}, \mathbf{a} \rangle$ or $\|\mathbf{x}'\|$ or the direction of \mathbf{x}' from the state $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle := \sum_{u' \in \mathbb{R}} \rho_{\sqrt{2}\sqrt{r^2\|\mathbf{x}'\|^2 + \sigma^2}}(u') \cdot e^{2\pi i \cdot u' \cdot \theta} |\langle \mathbf{s}, \mathbf{a} \rangle + u' \bmod q\rangle$ with measurement results \mathbf{a} and \mathbf{y} , where $\theta := \frac{r^2 \langle \mathbf{x}', \mathbf{y}'/R \rangle}{r^2\|\mathbf{x}'\|^2 + \sigma^2}$, $\mathbf{y}'/R := \mathbf{y}/R - \kappa_{(qL)^*}(\mathbf{y}/R)$. If this is done then using the reduction in [section 2.2](#) we can solve standard lattice problems via quantum algorithm.

3.1 Measuring the overlap of $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle$ and uniform to approximate $\|\mathbf{x}'\|$

Start with the case where $\mathbf{y} = \mathbf{0}$ and no phase is involved, then our state $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{0}}\rangle$ is displayed in [eq. \(4\)](#). An important observation is that when $\|\mathbf{x}'\|$ is small, the mass of $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{0}}\rangle$ is in a small range, while when $\|\mathbf{x}'\|$ is large, $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{0}}\rangle$ seems close to the uniform superposition $|\nu\rangle := \sum_{z \in \mathbb{Z}_q} |z\rangle$. Hence measuring the overlap between $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{0}}\rangle$ and $|nu\rangle$ reveals whether $\|\mathbf{x}'\|$ is small or large, which allows us to estimate $\|\mathbf{x}'\|$ within some precision.

Since the probability of getting $\mathbf{y} = \mathbf{0}$ is negligible¹, we need to take the phase into consideration. However, the distribution of θ in the phase is “neutralizing” the above effect: the expectation of $|\langle \psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}} | \nu \rangle|^2$ is independent of $\|\mathbf{x}'\|$.

This is not surprising since this overlap measurement does not use the measurement result \mathbf{y} , then measuring the second register should give the same result as measuring the second register of [eq. \(1\)](#), which is equivalent to measuring the overlap between the uniform superposition and a mixture of $\{\sum_{e \in \mathbb{R}} \rho_{\sqrt{2}\sigma}(e) |\langle \mathbf{x}, \mathbf{v} \rangle + e \bmod q\rangle\}_{\mathbf{v} \in qL + L\mathbf{a}}$, which is a constant depending on σ and q .

According to the above arguments, we need to find a way to utilize the information in the measurement result \mathbf{y} in order to extract information of \mathbf{x}' . Let's next figure out the distribution of \mathbf{y} , \mathbf{y}'/R and θ in our favourite state $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle$.

3.2 The distribution of \mathbf{y}

Now we give a more detailed analysis of the distribution of \mathbf{y} obtained by measuring the register $|\mathbf{y}\rangle$ in [eq. \(1\)](#):

$$\sum_{\mathbf{y} \in \mathbb{Z}_R^n} \sum_{\mathbf{v} \in qL + L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v}) \cdot \omega_R^{\langle \mathbf{v}, \mathbf{y} \rangle} |\mathbf{y}\rangle \otimes \sum_{e \in \mathbb{R}} \rho_{\sqrt{2}\sigma}(e) |\langle \mathbf{x}, \mathbf{v} \rangle + e \bmod q\rangle$$

Computing the reduced density matrix of the first register, we have the probability of measuring $\mathbf{y} \in \mathbb{Z}_R^n$ proportional to

¹attach evidence

$$\begin{aligned}
& \sum_{t \in [-\frac{q}{2}, \frac{q}{2})} \left| \sum_{\mathbf{v} \in qL + La} \rho_{\sqrt{2}r}(\mathbf{v}) \rho_{\sqrt{2}\sigma}(t - \langle \mathbf{x}, \mathbf{v} \rangle \bmod q) \cdot e^{2\pi i \cdot \langle \mathbf{v}, \frac{\mathbf{y}}{R} \rangle} \right|^2 \\
& \approx \sum_{t' \in [-\frac{q}{2}, \frac{q}{2})} \left| \sum_{\mathbf{v} \in qL + La} \rho_{\sqrt{2}r}(\mathbf{v}) \cdot e^{2\pi i \cdot \langle \mathbf{v}, \frac{\mathbf{y}}{R} \rangle} \rho_{\sqrt{2}\sigma}(t' - \langle \mathbf{x}', \mathbf{v} \rangle) \right|^2
\end{aligned} \tag{5}$$

where we can drop $\bmod q$ in the approximation since we set the parameters so that, with overwhelming probability over the randomness of e and \mathbf{v} , t' can be written as $t' = \langle \mathbf{x}', \mathbf{v} \rangle + e$ without $\bmod q$.

One can compute with a little effort that in eq. (5) the term associated with a fixed t' is

$$\begin{aligned}
& \sum_{\mathbf{v} \in qL + La} \rho_{\sqrt{2}r}(\mathbf{v}) \cdot e^{2\pi i \cdot \langle \mathbf{v}, \frac{\mathbf{y}}{R} \rangle} \rho_{\sqrt{2}\sigma}(t' - \langle \mathbf{x}', \mathbf{v} \rangle) \\
& = \sum_{\mathbf{v} \in qL + La} \rho_{\sqrt{2}\Sigma}(\mathbf{v} - \mathbf{m}_{t'}) \cdot e^{2\pi i \cdot \langle \mathbf{v}, \mathbf{y}/R \rangle} \\
& \stackrel{(1)}{=} \sum_{\mathbf{w} \in (qL)^*} \rho_{\sqrt{\Sigma^{-1}/2}}(\mathbf{w} - \mathbf{y}/R) \cdot e^{2\pi i \cdot \langle \mathbf{w}, La - \mathbf{m}_{t'} \rangle} \cdot e^{2\pi i \cdot \langle \mathbf{m}_{t'}, \mathbf{y}/R \rangle} \\
& \stackrel{(2)}{\approx} \rho_{\sqrt{\Sigma^{-1}/2}}(\mathbf{y}'/R) \cdot e^{2\pi i \cdot \langle \mathbf{w}, La - \mathbf{m}_{t'} \rangle} \cdot e^{2\pi i \cdot \langle \mathbf{m}_{t'}, \mathbf{y}/R \rangle}
\end{aligned} \tag{6}$$

where $\mathbf{m}_{t'} := \frac{r^2 t'}{r^2 \|\mathbf{x}'\|^2 + \sigma^2} \mathbf{x}'$, $\Sigma := r^2 I - \frac{r^4 \|\mathbf{x}'\|^2}{r^2 \|\mathbf{x}'\|^2 + \sigma^2}$, $\Sigma^{-1} = \frac{I}{r^2} + \frac{\|\mathbf{x}'\|^2}{\sigma^2}$ and $\rho_{\sqrt{\Sigma}}(\mathbf{z}) := e^{-\pi \mathbf{z}^T \Sigma^{-1} \mathbf{z}}$ (without normalization).

(1) in eq. (6) is due to the Poisson Summation Formula. (2) in eq. (6) can be proved by directly applying the generalized tail bound lemma 10 for multi-variate Gaussian, proved in the appendix, with Σ having two singular values r^2 and $r^2 \cdot \frac{\sigma^2}{r^2 \|\mathbf{x}'\|^2 + \sigma^2}$.

Hence, the distribution of \mathbf{y} is approximately proportional to $\rho_{\sqrt{\Sigma^{-1}/2}}(\mathbf{y}'/R)$ that only depends on \mathbf{y}' . Therefore the distribution of \mathbf{y}/R can be seen as ellipsoids centered at lattice points of $(qL)^*$ whose direction of major axes is \mathbf{x}' . Then the distribution of \mathbf{y}/R reveals two aspects of \mathbf{x}' :

1. The width of \mathbf{y}'/R is inversely related to $\|\mathbf{x}'\|$.
2. The shape of the support of \mathbf{y}/R is related to the direction of \mathbf{x}' . However these ellipsoids are cut by the boundaries of the cube $[-1/2, 1/2]^n$, leading to an troublesome support of \mathbf{y}/R .

Besides, one can argue that the distribution of \mathbf{y}'/R is proportional to

$$|(qL)^* + \mathbf{y}' \cap \mathbb{Z}_R^n| \cdot \rho_{\sqrt{\Sigma^{-1}/2}}(\mathbf{y}'/R)$$

If \mathbf{y}/R can be viewed as, say, an unbounded real number, then the distribution of \mathbf{y}'/R follows $\rho_{\sqrt{\Sigma^{-1}/2}}$ and hence $\|\mathbf{y}'\| < \sqrt{n} \cdot \frac{\sqrt{\sigma^2 + r^2 \|\mathbf{x}'\|^2}}{2\sigma r}$. However \mathbf{y}/R is actually within the cube $[-1/2, 1/2]^n$,

Remark 6. Unless there exists different \mathbf{y}'_1 and \mathbf{y}'_2 such that $\frac{|(qL)^* + \mathbf{y}'_1 \cap \mathbb{Z}_R^n|}{|(qL)^* + \mathbf{y}'_2 \cap \mathbb{Z}_R^n|} = O(2^n)$, we always have $\|\mathbf{y}'\| < \sqrt{n} \cdot \frac{\sqrt{\sigma^2 + r^2 \|\mathbf{x}'\|^2}}{2\sigma r}$ with overwhelming probability.

Assuming all $|(qL)^* + \mathbf{y}' \cap \mathbb{Z}_R^n|$ are approximately the same, then $\theta = \frac{r^2 \langle \mathbf{x}', \mathbf{y}'/R \rangle}{r^2 \|\mathbf{x}'\|^2 + \sigma^2}$ in the phase of the amplitude of $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle$ follows the Gaussian distribution ρ_β where $\beta := \frac{r \|\mathbf{x}'\|}{2\sigma \sqrt{r^2 \|\mathbf{x}'\|^2 + \sigma^2}}$.

3.3 Use \mathbf{y} when measuring $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle$

In the previous subsection we measure $|\psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}}\rangle$ by $|\nu\rangle$ and hope to extract the information about $\|\mathbf{x}'\|$. But $\mathbb{E}_{\mathbf{y}}(|\langle \psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}} | \nu \rangle|^2)$ is independent of \mathbf{x}' since we haven't used the information about \mathbf{y} at all.

The target. To understand where the information of \mathbf{y} can be useful, let us recall that the amplitude of $u' := \langle \mathbf{x}', \mathbf{v} \rangle + e = \langle \mathbf{x}', \mathbf{w} \rangle$ is

$$\rho_{\sqrt{2} \sqrt{r^2 \|\mathbf{x}'\|^2 + \sigma^2}}(u') \cdot e^{2\pi i \cdot u' \cdot \theta} \quad (7)$$

where $\theta = \frac{r^2 \langle \mathbf{x}', \mathbf{y}'/R \rangle}{r^2 \|\mathbf{x}'\|^2 + \sigma^2}$. For simplicity, let's first assume θ follows the Gaussian distribution ρ_β .

If we can change θ multiplicatively, say, let θ be c times the current θ for some $c \neq 1$ (c doesn't have to be a constant, c is not necessarily known, think of c as some number that is not equal to 1), meaning that θ follows $\rho_{c\beta}$, then $\mathbb{E}_{\mathbf{y}}(|\langle \psi_{\langle \mathbf{s}, \mathbf{a} \rangle, \mathbf{y}} | \nu \rangle|^2)$ depends on $\|\mathbf{x}'\|$.

The solution. (not closed) To change θ , we must add a phase that contains $\langle \mathbf{x}', \mathbf{y}'/R \rangle$. Here is one way to do so. The highlevel idea is:

1. First we assume we get a $\mathbf{y} \in L \cap \mathbb{Z}_R^n$ instead of $\mathbf{y} \in \mathbb{Z}_R^n$. This is easy to do as long as $\gcd(R, \det(L)) = 1$.
2. Then we compute $z := \langle \mathbf{x}, \mathbf{y} \rangle$. Since $\mathbf{y} \in L$, we have

$$\langle \mathbf{x}, \mathbf{y} \rangle = \langle \kappa_{L^*}(\mathbf{x}), \mathbf{y} \rangle + \langle \mathbf{x}', \mathbf{y} \rangle \in \mathbb{Z} + \langle \mathbf{x}', \mathbf{y} \rangle \in \mathbb{Z} + R \cdot \langle \mathbf{x}', \kappa_{(qL)^*}(\mathbf{y}/R) \rangle + R \cdot \langle \mathbf{x}', \mathbf{y}'/R \rangle,$$

$$\text{where } \mathbf{y}'/R \leq \sqrt{n} \cdot \frac{\sqrt{\sigma^2 + r^2 \|\mathbf{x}'\|^2}}{2\sigma r}.$$

3. In z we are left with two terms: $R \cdot \langle \mathbf{x}', \kappa_{(qL)^*}(\mathbf{y}/R) \rangle$ and $R \cdot \langle \mathbf{x}', \mathbf{y}'/R \rangle$. We want to let the first term disappear and make the second term with comparable size to $\frac{r^2 \langle \mathbf{x}', \mathbf{y}'/R \rangle}{r^2 \|\mathbf{x}'\|^2 + \sigma^2}$. The idea is to assume \mathbf{x}' only needs certain precision to represent (say, $\mathbf{x}' \in \mathbb{Z}^n / (r \cdot \ell)$, where $\ell \in O(n^\epsilon)$ for some $\epsilon > 0$), and $(qL)^*$ is a subset of $\mathbb{Z}^n / (qp)$ for some $p \in \mathbb{Z}$. Therefore we can multiply both terms by some $N \in \mathbb{Z}$ so that $NR \cdot \langle \mathbf{x}', \kappa_{(qL)^*}(\mathbf{y}/R) \rangle \in \mathbb{Z}$, and $NR \cdot \langle \mathbf{x}', \mathbf{y}'/R \rangle$ is of comparable size to $\frac{r^2 \langle \mathbf{x}', \mathbf{y}'/R \rangle}{r^2 \|\mathbf{x}'\|^2 + \sigma^2}$.
4. Then $N \cdot z \in \mathbb{Z} + NR \cdot \langle \mathbf{x}', \mathbf{y}'/R \rangle$. We let θ' be the one that drops in the integer part of Nz , i.e., let $\theta' := NR \cdot \langle \mathbf{x}', \mathbf{y}'/R \rangle$. Then we can create a phase of $e^{2\pi i u' \cdot \theta'}$.

The third step requires more assumptions, so let us add more details.

More details of Step 3. For $\theta = \frac{\langle \mathbf{x}', \mathbf{y}'/R \rangle \cdot (r/t)^2}{\|\mathbf{x}'\|^2}$, we know that

$$\frac{(r/t)^2}{\|\mathbf{x}'\|^2} = \frac{r^2 \|\mathbf{x}'\|^2}{r^2 \|\mathbf{x}'\|^2 + \sigma^2} \frac{1}{\|\mathbf{x}'\|^2} \in O\left(\frac{r^2}{(\alpha q)^2}\right)$$

4 Other possible methods

4.1 Bypassing |LWE⟩

The first attempt inspires us to use the distribution of our measurement results to recover useful information. Here we no longer insist on first reducing standard lattice problems to $\mathbf{S|LWE}$. In fact, we only need to give an algorithm that solves \mathbf{CVP} using polynomial discrete Gaussian states. Combining the algorithm with step 3 and step 4 of our plan, we can get an iterative algorithm for standard lattice problems.

Given an instance \mathbf{x} of \mathbf{CVP} , we begin with discrete Gaussian state

$$\sum_{\mathbf{v} \in L} \rho_{\sqrt{2}r}(\mathbf{v}) |\mathbf{v}\rangle$$

Again we measure $\mathbf{a} := L^{-1}\mathbf{v} \bmod q$ to get our favorite state

$$\sum_{\mathbf{v} \in qL + L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v}) |\mathbf{v}\rangle$$

We apply a unitary on the state to send $\langle \mathbf{x}, \mathbf{v} \rangle \bmod q$ to the phase and obtain

$$\sum_{\mathbf{v} \in qL + L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v}) \cdot e^{\frac{2\pi i \langle \mathbf{x}, \mathbf{v} \rangle}{q}} |\mathbf{v}\rangle \quad (8)$$

Apply \mathbf{QFT}_R for $R > r\sqrt{n}$ and we can get

$$|\psi\rangle := \sum_{\mathbf{y} \in \mathbb{Z}_R^n} \sum_{\mathbf{v} \in qL + L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v}) \cdot e^{2\pi i \frac{\langle \mathbf{x}, \mathbf{v} \rangle}{q}} \cdot e^{2\pi i \frac{\langle \mathbf{y}, \mathbf{v} \rangle}{R}} |\mathbf{y}\rangle \quad (9)$$

From Poisson summation formula,

$$|\psi\rangle = \sum_{\mathbf{y} \in \mathbb{Z}_R^n} \sum_{\mathbf{w} \in (qL)^*} \rho_{\frac{1}{\sqrt{2}r}}\left(\mathbf{w} - \frac{\mathbf{x}'}{q} - \frac{\mathbf{y}}{R}\right) \cdot e^{2\pi i \left(\langle \mathbf{w}, L\mathbf{a} \rangle + \frac{\langle \mathbf{s}, \mathbf{a} \rangle}{q}\right)} |\mathbf{y}\rangle \quad (10)$$

Then we measure $|\mathbf{y}\rangle$. The resulting vector \mathbf{y}/R , when parsed as a rational vector in $[-1/2, 1/2]^n$, is expected to stay with a radius of $\sqrt{n}/2r$ around $(qL)^* - \frac{\mathbf{x}'}{q}$.

Here is an intuitive idea of estimating \mathbf{x}' . We collect many samples of \mathbf{y}/R and then take the average. We expect the average to be $-\frac{\mathbf{x}'}{q}$, which is enough for solving \mathbf{CVP} .

Unfortunately, our intuition is not valid. To be more specific, when r is large, say exponential, then the length of the shift $\frac{\mathbf{x}'}{q}$ is less than $\frac{\alpha q}{r} \cdot \frac{1}{q} = \frac{\alpha}{r}$, which is negligible and can not be detected by efficient algorithms. We can also start from some special lattices such that initially r is small, say polynomial, but then the intersection between the boundary of $[-1/2, 1/2]^n$ and the balls of radius $\sqrt{n}/2r$ around $(qL)^* - \frac{\mathbf{x}'}{q}$ becomes annoying and thus the average of \mathbf{y}/R is not $-\frac{\mathbf{x}'}{q}$.

References

- [Ban93] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993. [8](#)
- [CLZ21] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. Cryptology ePrint Archive, Paper 2021/1093, 2021. <https://eprint.iacr.org/2021/1093>. [1](#)
- [GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008. [2](#)
- [Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009. [1](#), [2](#), [11](#)

A Appendix

A.1 An extension of Banaszczyk’s Gaussian tail bounds over lattices

Recall Banaszczyk’s Gaussian tail bounds:

Lemma 7 (Lemma 1.5 [Ban93]). *For any n -dimensional lattice L , $\mathbf{c} \in \mathbb{R}^n$, and $r \geq \frac{1}{\sqrt{2\pi}}$,*

$$\rho((L - \mathbf{c}) \setminus r\sqrt{n}B_2^n) < 2 \left(r\sqrt{2\pi}e \cdot e^{-\pi r^2} \right)^n \rho(L).$$

We extend this tail bounds’ RHS to an arbitrary shift of the lattice:

Lemma 8. *For any n -dimensional lattice L , such that $\lambda_1(L) > 3\sqrt{n}$, and any $\mathbf{y} \in \mathbb{R}^n$ such that $\text{dist}(\mathbf{y}, L) < \sqrt{n}$, we have*

$$\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n} \rho(L - \mathbf{y}). \quad (11)$$

Proof. First we prove that since $\lambda_1(L) > 3\sqrt{n}$, we have $\rho(L) < 1 + 2^{-n}$. To do so, we apply Lemma 7 with $\mathbf{c} = \mathbf{0}$ and $r\sqrt{n} = \lambda_1(L)/2$, which gives

$$\begin{aligned} \rho(L \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) &< 2 \left(\frac{\lambda_1(L)}{2\sqrt{n}} \sqrt{2\pi}e \cdot e^{-\pi \left(\frac{\lambda_1(L)}{2\sqrt{n}} \right)^2} \right)^n \cdot \rho(L) \\ &= 2 \cdot e^{n \ln(\lambda_1(L)/\sqrt{n}) - \pi \lambda_1(L)^2/4 + n \ln \sqrt{\pi e/2}} \cdot \rho(L) \end{aligned} \quad (12)$$

Let $\lambda_1(L) = x \cdot \sqrt{n}$, then consider the function

$$f(x) := \ln(x) - \pi x^2/4 + \ln(\sqrt{\pi e/2}) \quad (13)$$

The derivative of f is

$$f'(x) = 1/x - \pi x/2 \quad (14)$$

Therefore when $x > \sqrt{2/\pi}$, f is decreasing. When $x > 3$, $f(x) < -5.24$.

Hence if $\lambda_1(L) > 3\sqrt{n}$,

$$\rho(L \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2 \cdot e^{-5.24n} \cdot \rho(L),$$

which means $\rho(L) < 1 + 2^{-n}$

We continue proving Lemma 8 by applying Lemma 7 with $\mathbf{c} = \mathbf{y}$ and $r\sqrt{n} = \lambda_1(L)/2$. This gives

$$\begin{aligned} \rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) &< 2 \left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}} \right)^n \cdot e^{-\pi\lambda_1(L)^2/4} \rho(L) \\ &<_{(1)} 3 \left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}} \right)^n \cdot e^{-\pi\lambda_1(L)^2/4} \end{aligned} \quad (15)$$

where (1) uses $\rho(L) < 1 + 2^{-n}$.

Let $\mathbf{y}' = \mathbf{y} - \kappa_L(\mathbf{y})$, then $\|\mathbf{y}'\| = \text{dist}(\mathbf{y}, L) < \sqrt{n}$. Then

$$\begin{aligned} \frac{\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n)}{\rho(\mathbf{y}')} &< 3e^{n \ln\left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}}\right) - \pi\lambda_1(L)^2/4 + \pi\|\mathbf{y}'\|^2} \\ &< 3e^{n \ln(\lambda_1(L)/\sqrt{n}) - \pi\lambda_1(L)^2/4 + n\pi + n \ln \sqrt{\pi e/2}} \\ &<_{(1)} 3e^{n \ln(3) - \frac{9}{4}n\pi + n\pi + n \ln \sqrt{\pi e/2}} \\ &= 3e^{n(\ln 3 - \frac{5}{4}\pi + \ln \sqrt{\pi e/2})}, \end{aligned} \quad (16)$$

where (1) is obtained by taking the derivative similar as before: let $\lambda_1(L) = x \cdot \sqrt{n}$, then consider the function

$$g(x) := \ln(x) - \pi x^2/4 + \ln(\sqrt{\pi e/2}) + \pi \quad (17)$$

The derivative of g is

$$g'(x) = 1/x - \pi x/2 \quad (18)$$

Therefore when $x > \sqrt{2/\pi}$, g is decreasing. When $x > 3$, $g(x) < -2.1$.

Hence when $\lambda_1(L) > 3\sqrt{n}$ and $\|\mathbf{y}'\| < \sqrt{n}$,

$$\frac{\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n)}{\rho(\mathbf{y}')} < 2^{-2n}.$$

Since $\rho(L - \mathbf{y}) = \rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) + \rho(\mathbf{y}')$, we have

$$\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n} \rho(L - \mathbf{y}). \quad (19)$$

□

For technical reason, we need a variant of lemma 8:

Lemma 9. For any n -dimensional lattice L and any $\mathbf{y} \in \mathbb{R}^n$, such that $\lambda_1(L) > 3\text{dist}(\mathbf{y}, L)/d$ and $\lambda_1(L) > 3\sqrt{n}$, we have

$$\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n} \rho_d(L - \mathbf{y}). \quad (20)$$

Remark: we can treat d as minor axis / major axis, which is less than 1.

Proof. First we prove that since $\lambda_1(L) > 3\sqrt{n}$, we have $\rho(L) < 1 + 2^{-n}$. To do so, we apply Lemma 7 with $\mathbf{c} = \mathbf{0}$ and $r\sqrt{n} = \lambda_1(L)/2$, which gives

$$\begin{aligned} \rho(L \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) &< 2 \left(\frac{\lambda_1(L)}{2\sqrt{n}} \sqrt{2\pi e} \cdot e^{-\pi \left(\frac{\lambda_1(L)}{2\sqrt{n}} \right)^2} \right)^n \cdot \rho(L) \\ &= 2 \cdot e^{n \ln(\lambda_1(L)/\sqrt{n}) - \pi \lambda_1(L)^2/4 + n \ln \sqrt{\pi e/2}} \cdot \rho(L) \end{aligned} \quad (21)$$

Let $\lambda_1(L) = x \cdot \sqrt{n}$, then consider the function

$$f(x) := \ln(x) - \pi x^2/4 + \ln(\sqrt{\pi e/2}) \quad (22)$$

The derivative of f is

$$f'(x) = 1/x - \pi x/2 \quad (23)$$

Therefore when $x > \sqrt{2/\pi}$, f is decreasing. When $x > 3$, $f(x) < -5.24$.

Hence if $\lambda_1(L) > 3\sqrt{n}$,

$$\rho(L \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2 \cdot e^{-5.24n} \cdot \rho(L),$$

which means $\rho(L) < 1 + 2^{-n}$

We continue proving Lemma 9 by applying Lemma 7 with $\mathbf{c} = \mathbf{y}$ and $r\sqrt{n} = \lambda_1(L)/2$. This gives

$$\begin{aligned} \rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) &< 2 \left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}} \right)^n \cdot e^{-\pi \lambda_1(L)^2/4} \rho(L) \\ &<_{(1)} 3 \left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}} \right)^n \cdot e^{-\pi \lambda_1(L)^2/4} \end{aligned} \quad (24)$$

where (1) uses $\rho(L) < 1 + 2^{-n}$.

Let $\mathbf{y}' = \mathbf{y} - \kappa_L(\mathbf{y})$, then $\|\mathbf{y}'\|/d = \text{dist}(\mathbf{y}, L)/d < \lambda_1(L)/3$. Then

$$\begin{aligned} \frac{\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n)}{\rho_d(\mathbf{y}')} &< 3e^{n \ln \left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}} \right) - \pi \lambda_1(L)^2/4 + \pi \|\mathbf{y}'\|^2/d^2} \\ &< 3e^{n \ln(\lambda_1(L)/\sqrt{n}) - \pi \lambda_1(L)^2/4 + \pi \lambda_1(L)^2/9 + n \ln \sqrt{\pi e/2}} \\ &<_{(1)} 3e^{n \ln(3) - \frac{9}{4}n\pi + n\pi + n \ln \sqrt{\pi e/2}} \\ &= 3e^{n(\ln 3 - \frac{5}{4}\pi + \ln \sqrt{\pi e/2})}, \end{aligned} \quad (25)$$

where (1) is obtained by taking the derivative similar as before: let $\lambda_1(L) = x \cdot \sqrt{n}$, then consider the function

$$g(x) := \ln(x) - 5\pi x^2/36 + \ln(\sqrt{\pi e/2}) \quad (26)$$

The derivative of g is

$$g'(x) = 1/x - 5\pi x/18 \quad (27)$$

Therefore when $x > \sqrt{\frac{18}{5\pi}}$, g is decreasing. When $x > 3$, $g(x) < -2.1$.

Hence when $\lambda_1(L) > 3\text{dist}(\mathbf{y}, L)/d$ and $\lambda_1(L) > 3\sqrt{n}$,

$$\frac{\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n)}{\rho_d(\mathbf{y}')} < 2^{-2n}.$$

Since $\rho_d(L - \mathbf{y}) = \rho_d((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) + \rho_d(\mathbf{y}')$, we have

$$\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n} \rho_d(L - \mathbf{y}). \quad (28)$$

□

Corollary 10. *For any n -dimensional lattice L , any $y \in \mathbb{R}^n$ and any symmetric and positive matrix Σ whose smallest singular value is a^2 and whose largest singular value is b^2 , such that $\lambda_1(L) > \frac{3b}{a}\text{dist}(\mathbf{y}, L)$ and $\lambda_1(L) > 3\sqrt{n}/a$, we have*

$$\rho_\Sigma((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) \leq \rho_{\frac{1}{a}}((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n} \rho_{\frac{1}{b}}(L - \mathbf{y}) \leq 2^{-n} \rho_\Sigma(L - \mathbf{y}). \quad (29)$$

A.2 Smoothing of Gaussian with a phase

We generalize [Reg09, Claim 3.9] to handle Gaussian function with a phase.

Theorem 11. *Let L be a lattice, $\mathbf{u} \in \mathbb{R}^n$ be any vector, $r, s > 0$ be any real numbers, $t := \sqrt{r^2 + s^2}$. Consider the function Y on $\mathbf{x} \in \mathbb{R}^n$ as the convolution of*

1. \mathbf{y} with support $L + \mathbf{u}$ and amplitude $h(\mathbf{y}) := \rho_r(\mathbf{y}) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle}$ for some fixed $\mathbf{z} \in \mathbb{R}^n$ such that $d(\mathbf{z}, L^*) < \frac{t}{rs} \sqrt{n}$;
2. A noise vector taken from ρ_s .

Suppose $\frac{rs}{t} \lambda_1(L^*) > 3\sqrt{n}$. Then $Y(\mathbf{x}) \approx \rho_t(\mathbf{x}) \cdot e^{2\pi i \cdot (r/t)^2 \langle \mathbf{z} - \kappa_{L^*}(\mathbf{z}), \mathbf{x} \rangle}$.

Proof. The function Y can be written as

$$\begin{aligned} Y(\mathbf{x}) &= \sum_{\mathbf{y} \in L + \mathbf{u}} h(\mathbf{y}) \rho_s(\mathbf{x} - \mathbf{y}) \\ &= \sum_{\mathbf{y} \in L + \mathbf{u}} \exp\left(-\pi \left(\frac{\|\mathbf{y}\|^2}{r^2} + \frac{\|\mathbf{x} - \mathbf{y}\|^2}{s^2} \right)\right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle} \\ &= \exp\left(-\frac{\pi}{r^2 + s^2} \|\mathbf{x}\|^2\right) \sum_{\mathbf{y} \in L + \mathbf{u}} \exp\left(-\pi \left(\frac{t}{rs} \right)^2 \cdot \left\| \mathbf{y} - \frac{r^2}{t^2} \mathbf{x} \right\|^2\right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle} \\ &= \rho_t(\mathbf{x}) \cdot \sum_{\mathbf{y} \in L + \mathbf{u}} \exp\left(-\pi \left(\frac{t}{rs} \right)^2 \cdot \left\| \mathbf{y} - \frac{r^2}{t^2} \mathbf{x} \right\|^2\right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle} \end{aligned} \quad (30)$$

For any $\mathbf{y} \in \mathbb{R}^n$, let $g(\mathbf{y}) := \rho_{\frac{rs}{t}}(\mathbf{y}) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle}$. Then

$$\hat{g}(\mathbf{w}) = \rho_{\frac{t}{rs}}(\mathbf{w} - \mathbf{z})$$

Then

$$\begin{aligned} & \sum_{\mathbf{y} \in L + \mathbf{u}} \exp \left(-\pi \left(\frac{t}{rs} \right)^2 \cdot \left\| \mathbf{y} - \frac{r^2}{t^2} \mathbf{x} \right\|^2 \right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle} \\ &= \sum_{\mathbf{y} \in L} \rho_{\frac{rs}{t}} \left(\mathbf{y} + \mathbf{u} - \frac{r^2}{t^2} \mathbf{x} \right) \cdot e^{2\pi i \cdot \langle \mathbf{y} + \mathbf{u}, \mathbf{z} \rangle} \\ &= \sum_{\mathbf{y} \in L} g(\mathbf{y} + \mathbf{u} - \frac{r^2}{t^2} \mathbf{x}) \cdot e^{2\pi i \cdot \langle \frac{r^2}{t^2} \mathbf{x}, \mathbf{z} \rangle} \\ &=_{(1)} \sum_{\mathbf{w} \in L^*} \hat{g}(\mathbf{w}) \cdot e^{2\pi i \cdot \langle \mathbf{u} - (r/t)^2 \mathbf{x}, \mathbf{w} \rangle} \cdot e^{2\pi i \cdot \langle \frac{r^2}{t^2} \mathbf{x}, \mathbf{z} \rangle} \\ &= \sum_{\mathbf{w} \in L^*} \rho_{t/rs}(\mathbf{w} - \mathbf{z}) \cdot e^{2\pi i \cdot (\langle \mathbf{u}, \mathbf{w} \rangle - \langle (r/t)^2 \mathbf{x}, \mathbf{w} - \mathbf{z} \rangle)} \end{aligned} \quad (31)$$

where (1) uses Poisson Summation Formula (ignoring the normalization factor $(rs/t)^n \det(L^*)$).

Applying Lemma 8 with the lattice L being $\frac{rs}{t}L^*$ here, which is $\frac{rs}{t}(qL)^*$ in the main theorem; the vector \mathbf{y} being $\frac{rs}{t} \cdot \mathbf{z}$, which is $\frac{rs}{t} \cdot \frac{\mathbf{y}}{R}$ in the main theorem; $\lambda_1(L)$ being $\frac{rs}{t}\lambda_1(L^*)$ here, which is $\frac{rs}{tq}\lambda_1(L^*)$ in the main theorem.

Recall that $s\|\mathbf{x}'\| = \sigma$ and $t = \sqrt{r^2 + s^2}$. $\text{dist}(\mathbf{y}, L)$ in Lemma 8 satisfies

$$\text{dist}(\mathbf{y}, L) < \sqrt{n} \cdot \frac{\sqrt{\sigma^2 + r^2\|\mathbf{x}'\|^2}}{\sigma r} \cdot \frac{rs}{t} = \sqrt{n} \cdot \frac{\sqrt{(s\|\mathbf{x}'\|)^2 + r^2\|\mathbf{x}'\|^2}}{s\|\mathbf{x}'\|r} \cdot \frac{rs}{\sqrt{r^2 + s^2}} = \sqrt{n}$$

Back to Eqn. (31), when $\frac{rs}{t} > \frac{3\sqrt{n}}{\lambda_1(L^*)}$ and $\|\mathbf{z}'\| < \frac{t\sqrt{n}}{rs}$ with $\mathbf{z}' := \mathbf{z} - \kappa_{L^*}(\mathbf{z})$, we have

$$\sum_{\mathbf{w} \in L^*} \rho_{t/rs}(\mathbf{w} - \mathbf{z}) \cdot e^{2\pi i \cdot (\langle \mathbf{u}, \mathbf{w} \rangle - \langle (r/t)^2 \mathbf{x}, \mathbf{w} - \mathbf{z} \rangle)} \approx \rho_{t/rs}(\mathbf{z}') \cdot e^{2\pi i \cdot (\langle \mathbf{u}, \kappa_{L^*}(\mathbf{z}) \rangle + \langle (r/t)^2 \mathbf{x}, \mathbf{z}' \rangle)} \quad (32)$$

Then $Y(\mathbf{x}) \propto \rho_t(\mathbf{x}) \cdot e^{2\pi i \cdot (r/t)^2 \langle \mathbf{z} - \kappa_{L^*}(\mathbf{z}), \mathbf{x} \rangle}$.

□

A.3 Linear combination of continuous Gaussian with a phase

Theorem 12. For any $\mathbf{x} \in \mathbb{R}^n$ such that $\|\mathbf{x}\| > 0$. Suppose the amplitude of $\mathbf{v} \in \mathbb{R}^n$ is $f(\mathbf{v}) = \rho_r(\mathbf{v}) \cdot e^{2\pi i \cdot (\langle \mathbf{v}, \mathbf{y} \rangle + w)}$ for some fixed $\mathbf{y} \in \mathbb{R}^n$ and $w \in \mathbb{R}$, then the amplitude of $u := \langle \mathbf{x}, \mathbf{v} \rangle$ is

$$g(u) = \lambda \cdot \rho_{\|\mathbf{x}\| \cdot r}(u) \cdot e^{2\pi i \cdot u \cdot \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2}}. \quad (33)$$

where λ is some fixed complex number.

Proof. Let $\mathbf{v}' \in \mathbb{R}^n$ be any real vector such that $\langle \mathbf{v}', \mathbf{y} \rangle = w$. Then the amplitude of $\mathbf{v} \in \mathbb{R}^n$ can be written as

$$f(\mathbf{v}) = \rho_r(\mathbf{v}) \cdot e^{2\pi i \langle \mathbf{v} + \mathbf{v}', \mathbf{y} \rangle} \quad (34)$$

For $j \in [n]$, let g_j denote the amplitude of $u_j := x_j \cdot v_j$. Then, when $x_j = 0$, $g_j = \delta_0 \cdot e^{2\pi i \cdot v'_j \cdot y_j}$, where δ denotes the indicator function; when $x_j \neq 0$,

$$g_j(u_j) = \rho_{x_j \cdot r}(u_j) \cdot e^{2\pi i \cdot (u_j \cdot y_j / x_j) + v'_j \cdot y_j} \quad (35)$$

Then the Fourier transform of g_j is

$$\hat{g}_j(z) = \begin{cases} e^{2\pi i \cdot v'_j \cdot y_j} & \text{when } x_j = 0; \\ e^{-\pi r^2 (x_j \cdot z - y_j)^2} \cdot e^{2\pi i \cdot v'_j \cdot y_j} & \text{when } x_j \neq 0; \end{cases} \quad (36)$$

So the product of $\hat{g}_1, \dots, \hat{g}_n$ is

$$\hat{g}(z) := \prod_{j=1}^n \hat{g}_j(z) = e^{-\pi r^2 (\|\mathbf{x}\|^2 \cdot z^2 - 2\langle \mathbf{x}, \mathbf{y} \rangle \cdot z + \delta)} \cdot e^{2\pi i \cdot w} = e^{-\pi r^2 \|\mathbf{x}\|^2 \cdot (z - \theta)^2 + \delta'} \cdot e^{2\pi i \cdot w} \quad (37)$$

where δ and δ' are some real numbers that does not depend on \mathbf{x} , $\theta = \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2}$ is a real number that depends on \mathbf{x} .

Then the amplitude of $u := \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{R}$ is the convolution of g_j , which is the Fourier transform of \hat{g} . So the amplitude of u is

$$g(u) = \hat{g}(u) = \lambda \cdot \rho_{\|\mathbf{x}\| \cdot r}(u) \cdot e^{2\pi i \cdot u \cdot \theta}. \quad (38)$$

where λ is some fixed complex number. □