Attempts to Quantumly Solve Standard Lattice Problems: Reduction from Standard Lattice Problems to $\mathsf{S}|\mathsf{LWE}\rangle$ and Beyond

Zihan Hu, Yaxin Tu (Authors of this note)
Yilei Chen (Dear advisor)
Qipeng Liu (Dear collaborator)

December 21, 2022

Contents

1 Introduction

In this note, we summarize our partial results on quantumly solving standard lattice problems.

Solving standard lattice problems has been a target for designing efficient quantum algorithms for decades. Regev [Reg09] shows given a polynomial time algorithm that solves $\mathsf{LWE}_{n,m,q,\mathcal{D}_{\mathsf{noise}}}$ where $\mathcal{D}_{\mathsf{noise}}$ is Gaussian and m can be any polynomial, one can construct a quantum algorithm that solves standard lattice problems.

Here let us consider the following quantum variant of the LWE problem called solving LWE given LWE-like states ($\mathsf{S}|\mathsf{LWE}\rangle$).

Definition 1 (Solving LWE given LWE-like quantum states ($\mathsf{S}|\mathsf{LWE}\rangle$))**.** *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* $\mathsf{S}|\mathsf{LWE}\rangle_{n,m,q,f}$ *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 $i = 1, ..., m$. Here each a_i is a uniformly random vector in $\mathbb{Z}_q^n$.*

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

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

2 Quantum reduction from Standard Lattice Problems to $\mathsf{S}|\mathsf{LWE}\rangle$

In this section, we'll show how to obtain a quantum reduction from standard lattice problems to $\mathsf{S}|\mathsf{LWE}\rangle$, by modifying Regev's reduction.

2.1 Summary of Regev's reduction [Reg09]

Let's start by recalling the details of Regev's reduction. Many standard lattice problems 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 $\mathsf{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$, using $\mathsf{poly}(n)$ 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 $\mathsf{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$ problem:

Theorem 3 ([Reg09]). *Suppose $m \in \mathsf{poly}(n)$, 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 $\epsilon \in \mathsf{negl}(n)$. There exists an efficient (classical) algorithm that, given an oracle that solves $\mathsf{LWE}_{n,m,q,q\Psi_\alpha}$ and $\mathsf{poly}(n,m)$ samples from $D_{L,r}$, solves $\mathsf{CVP}_{L^*,\alpha q/(\sqrt{2}r)}$, where Ψ_α denotes the periodic Gaussian distribution and $q\Psi_\alpha$ stands for scaling it by q.*

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

Theorem 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 $\mathsf{CVP}_{L^*,d}$, 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 $D_{L,r\cdot\sqrt{n}/(\alpha q)}$, 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 $\mathsf{S}|\mathsf{LWE}\rangle$ solver. The procedure is as follows:

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

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

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

Step 3 appears in case the $\mathsf{S}|\mathsf{LWE}\rangle$ solver in step 1 needs 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 $\mathsf{S}|\mathsf{LWE}\rangle$ oracle we require.

Let $\mathbf{x}$ denote a $\mathsf{CVP}_{L^*,\alpha q/r}$ 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 $|\mathsf{LWE}\rangle$ 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

$$\sum_{\mathbf{v}\in qL+L\mathbf{a}}\rho_{r\sqrt{2}}(\mathbf{v})|\mathbf{v}\rangle\otimes\sum_{e\in\mathbb{R}}\rho_{\sqrt{2}\sigma}(e)|\langle\mathbf{s},\mathbf{a}\rangle+\langle\mathbf{x}',\mathbf{v}\rangle+e \bmod q\rangle \tag{1}$$

   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:

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

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

$$\sum_{\mathbf{v}\in qL+L\mathbf{a}}\sum_{e\in\mathbb{R}}\rho_{r\sqrt{2}}(\mathbf{v})\rho_{\sqrt{2}\sigma}(e)\cdot\omega_R^{\langle\mathbf{v},\mathbf{y}\rangle}|\langle\mathbf{s},\mathbf{a}\rangle+\langle\mathbf{x}',\mathbf{v}\rangle+e \bmod q\rangle. \tag{3}$$

   According to Theorem 11, this state is close to:

$$|\psi_{\langle\mathbf{s},\mathbf{a}\rangle,\mathbf{y}}\rangle:=\sum_{u'\in\mathbb{R}}\rho_{\sqrt{2}\sqrt{r^2\|\mathbf{x}'\|^2+\sigma^2}}(u')\cdot e^{2\pi i\cdot u'\cdot\theta}|\langle\mathbf{s},\mathbf{a}\rangle+u' \bmod q\rangle, \tag{4}$$

   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 $|\mathsf{LWE}\rangle$ with error distribution being Gaussian distribution with a phase, then one can solve the $\mathsf{CVP}_{L^*,\alpha q/r}$ problem.

One caveat is this $\mathsf{S}|\mathsf{LWE}\rangle_{n,m,q,f}$ 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 4. 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*

$$\sum_{e' \in \mathbb{R}} \rho_{\sqrt{2}\sqrt{r^2\|\mathbf{x}'\|^2+\sigma^2}}(e') | \langle \mathbf{s}, \mathbf{a} \rangle + e' \bmod q \rangle, \tag{5}$$

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

3 Extracting secrets from $|\mathsf{LWE}\rangle$ 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 Equation (5). 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 negligible[1], 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 $\|x'\|$.

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 Equation (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 $\mathbf{x}'$. To better utilize $\mathbf{y}$, let's first 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 y

Now we give a more detailed analysis of the distribution of $\mathbf{y}$ obtained by measuring the register $|\mathbf{y}\rangle$ in (Equation (2)):

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

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

[1] Actually the distribution of $\mathbf{y}$ is approximately proportional to $\rho_{\sqrt{\Sigma^{-1}}/2}(\mathbf{y}'/R)$. See Section 3.2 for more detail.

$$
\begin{aligned}
&\sum_{t\in[-\frac{q}{2},\frac{q}{2})} \Big| \sum_{\mathbf{v}\in qL+L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v})\rho_{\sqrt{2}\sigma}(t-\langle \mathbf{x},\mathbf{v}\rangle \bmod q)\cdot e^{2\pi i\cdot\left\langle \mathbf{v},\frac{\mathbf{y}}{R}\right\rangle}\Big|^2 \\
\approx &\sum_{t'\in[-\frac{q}{2},\frac{q}{2})} \Big| \sum_{\mathbf{v}\in qL+L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v})\cdot e^{2\pi i\cdot\left\langle \mathbf{v},\frac{\mathbf{y}}{R}\right\rangle}\rho_{\sqrt{2}\sigma}(t'-\left\langle \mathbf{x}',\mathbf{v}\right\rangle)\Big|^2
\end{aligned}
\tag{6}
$$

where we can drop mod 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 mod q.

One can compute with a little effort that in Equation (6) the term associated with a fixed t' is

$$
\begin{aligned}
&\sum_{\mathbf{v}\in qL+L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v})\cdot e^{2\pi i\cdot\left\langle \mathbf{v},\frac{\mathbf{y}}{R}\right\rangle}\rho_{\sqrt{2}\sigma}(t'-\left\langle \mathbf{x}',\mathbf{v}\right\rangle) \\
= &\sum_{\mathbf{v}\in qL+L\mathbf{a}} \rho_{\sqrt{2\Sigma}}(\mathbf{v}-\mathbf{m}_{t'})\cdot e^{2\pi i\cdot\langle \mathbf{v},\mathbf{y}/R\rangle} \\
=_{(1)} &\sum_{\mathbf{w}\in(qL)^*} \rho_{\sqrt{\Sigma^{-1}/2}}(\mathbf{w}-\mathbf{y}/R)\cdot e^{2\pi i\langle \mathbf{w},L\mathbf{a}-\mathbf{m}_{t'}\rangle}\cdot e^{2\pi i\cdot\langle \mathbf{m}_{t'},\mathbf{y}/R\rangle} \\
\approx_{(2)} &\ \rho_{\sqrt{\Sigma^{-1}/2}}(\mathbf{y}'/R)\cdot e^{2\pi i\left\langle \kappa_{(qL)^*}(\mathbf{y}/R),L\mathbf{a}-\mathbf{m}_{t'}\right\rangle}\cdot e^{2\pi i\cdot\langle \mathbf{m}_{t'},\mathbf{y}/R\rangle}
\end{aligned}
\tag{7}
$$

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

(1) in Equation (7) is due to the Poisson Summation Formula. (2) in Equation (7) can be proved by directly applying the generalized tail bound Corollary 9 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 $\mathbf{x}'$.

Moreover, one can prove that $|(qL)^* + \mathbf{y}'/R \cap \mathbb{Z}_R^n|$ is the same for all $\mathbf{y}'/R$, since $(qL)^*$ is a suplattice of $\frac{1}{q}\mathbb{Z}^n$ and therefore the cube $[-1/2, 1/2)^n$ can be viewed as containing an integer number of parallelepiped $\mathcal{P}((qL)^*)$. Hence, the distribution of $\mathbf{y}'/R$ is proportional to $\rho_{\sqrt{\Sigma^{-1}}/2}(\mathbf{y}'/R)$, i.e., $\mathbf{y}'/R$ follows a multivariate Gaussian distribution. So we can bound the length of $\mathbf{y}'/R$:

$$
\|\mathbf{y}'\|/R \le \sqrt{n}\cdot\frac{\sqrt{r^2\|\mathbf{x}'\|^2+\sigma^2}}{2\sigma r}
\tag{8}
$$

It follows that $\theta = \frac{r^2\langle \mathbf{x}',\mathbf{y}'/R\rangle}{r^2\|\mathbf{x}'\|^2+\sigma^2}$ 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 Where can we find the secret?

Observe that the distribution of $\mathbf{y}/R$ contains the information we want. To be more specific, the shape of the support of $\mathbf{y}/R$ can be seen as ellipsoids centered at lattice points of $(qL)^*$, and the direction and the length of their major axes are related to $\mathbf{x}'$. It seems plausible that we can utilize $\mathbf{y}$ by extracting information about the secret from the distribution of $\mathbf{y}/R$.

In fact, the distribution of $\mathbf{y}/R$, $\mathbf{y}'/R$ and θ all contains information about $\mathbf{x}'$:

1. The width of $\mathbf{y}'/R$ is inversely related to $\|\mathbf{x}'\|$. However $\mathbf{y}'/R$ cannot be obtained directly. (Obtaining $\mathbf{y}'/R$ from $\mathbf{y}$ is an instance of $\mathsf{CVP}_{L^*, \frac{q\sqrt{n}\sqrt{\sigma^2+\alpha^2 q^2}}{2\sigma r}}$, which is harder than the $\mathsf{CVP}_{L^*,\alpha q/r}$ problem we're aiming to solve.)
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 a troublesome support of $\mathbf{y}/R$.
3. The width of the distribution of θ is positively related to $\|\mathbf{x}'\|$. However θ cannot be obtained directly either.

4 Bypassing $|\mathsf{LWE}\rangle$

The above 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 $\mathsf{S}|\mathsf{LWE}\rangle$. In fact, we only need to give an algorithm that solves CVP using polynomial discrete Gaussian states. Combining the algorithm with step 2 and step 3 of our plan, we can get an iterative algorithm for standard lattice problems.

Given an instance $\mathbf{x}$ of 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

$$\sum_{\mathbf{v}\in qL+L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v}) \cdot e^{\frac{2\pi i\langle \mathbf{x},\mathbf{v}\rangle}{q}}|\mathbf{v}\rangle \tag{9}$$

Apply QFT_R for $R > r\sqrt{n}$ and we can get

$$|\psi\rangle := \sum_{\mathbf{y}\in\mathbb{Z}_R^n} \sum_{\mathbf{v}\in qL+L\mathbf{a}} \rho_{\sqrt{2}r}(\mathbf{v}) \cdot e^{2\pi i\frac{\langle \mathbf{x},\mathbf{v}\rangle}{q}} \cdot e^{2\pi i\frac{\langle \mathbf{y},\mathbf{v}\rangle}{R}}|\mathbf{y}\rangle \tag{10}$$

From Poisson summation formula,

$$|\psi\rangle = \sum_{\mathbf{y}\in\mathbb{Z}_R^n} \sum_{\mathbf{w}\in(qL)^*} \rho_{\frac{1}{\sqrt{2}r}}\left(\mathbf{w} - \frac{\mathbf{x}'}{q} - \frac{\mathbf{y}}{R}\right) \cdot e^{2\pi i\left(\langle \mathbf{w},L\mathbf{a}\rangle + \frac{\langle \mathbf{s},\mathbf{a}\rangle}{q}\right)}|\mathbf{y}\rangle \tag{11}$$

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 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. 7

[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, 10

A Appendix

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

Recall Banaszczyk's Gaussian tail bounds:

Lemma 6 (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 aribitrary shift of the lattice:

Lemma 7. *For any n-dimensional lattice L, such that $\lambda_1(L) > 3\sqrt{n}$, and any $\mathbf{y} \in \mathbb{R}^n$ such that $dist(\mathbf{y}, L) < \sqrt{n}$, we have*

$$\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n}\rho(L - \mathbf{y}). \tag{12}$$

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 6 with $\mathbf{c} = \mathbf{0}$ and $r\sqrt{n} = \lambda_1(L)/2$, which gives

$$\begin{aligned}\rho(L \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) &< 2\left(\frac{\lambda_1(L)}{2\sqrt{n}}\sqrt{2\pi e} \cdot e^{-\pi\left(\frac{\lambda_1(L)}{2\sqrt{n}}\right)^2}\right)^n \cdot \rho(L) \\ &= 2 \cdot e^{n\ln(\lambda_1(L)/\sqrt{n}) - \pi\lambda_1(L)^2/4 + n\ln\sqrt{\pi e/2}} \cdot \rho(L)\end{aligned} \tag{13}$$

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

$$f(x) := \ln(x) - \pi x^2/4 + \ln(\sqrt{\pi e/2}) \tag{14}$$

The derivative of f is

$$f'(x) = 1/x - \pi x/2 \tag{15}$$

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 7 by applying Lemma 6 with $\mathbf{c} = \mathbf{y}$ and $r\sqrt{n} = \lambda_1(L)/2$. This gives

$$\begin{aligned}\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < &\ 2\left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}}\right)^n \cdot e^{-\pi\lambda_1(L)^2/4}\rho(L) \\ <_{(1)} &\ 3\left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}}\right)^n \cdot e^{-\pi\lambda_1(L)^2/4}\end{aligned} \tag{16}$$

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

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

$$\begin{aligned}\frac{\rho((L - \mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n)}{\rho(\mathbf{y}')} &< \ 3e^{n\ln\left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}}\right) - \pi\lambda_1(L)^2/4 + \pi\|\mathbf{y}'\|^2} \\ &< \ 3e^{n\ln(\lambda_1(L)/\sqrt{n}) - \pi\lambda_1(L)^2/4 + n\pi + n\ln\sqrt{\pi e/2}} \\ &< \ _{(1)}3e^{n\ln(3) - \frac{9}{4}n\pi + n\pi + n\ln\sqrt{\pi e/2}} \\ &= \ 3e^{n(\ln 3 - \frac{5}{4}\pi + \ln\sqrt{\pi e/2})},\end{aligned} \tag{17}$$

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

$$g(x) := \ln(x) - \pi x^2/4 + \ln(\sqrt{\pi e/2}) + \pi \tag{18}$$

The derivative of g is

$$g'(x) = 1/x - \pi x/2 \tag{19}$$

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

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

□

For technical reasons, we need a variant of Lemma 7:

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

$$\rho((L-\mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n}\rho_d(L-\mathbf{y}). \tag{21}$$

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 6 with $\mathbf{c} = \mathbf{0}$ and $r\sqrt{n} = \lambda_1(L)/2$, which gives

$$\begin{aligned}\rho(L \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) &< 2\left(\frac{\lambda_1(L)}{2\sqrt{n}}\sqrt{2\pi e} \cdot e^{-\pi\left(\frac{\lambda_1(L)}{2\sqrt{n}}\right)^2}\right)^n \cdot \rho(L) \\ &= 2 \cdot e^{n\ln(\lambda_1(L)/\sqrt{n}) - \pi\lambda_1(L)^2/4 + n\ln\sqrt{\pi e/2}} \cdot \rho(L)\end{aligned} \tag{22}$$

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

$$f(x) := \ln(x) - \pi x^2/4 + \ln(\sqrt{\pi e/2}) \tag{23}$$

The derivative of f is

$$f'(x) = 1/x - \pi x/2 \tag{24}$$

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 6 with $\mathbf{c} = \mathbf{y}$ and $r\sqrt{n} = \lambda_1(L)/2$. This gives

$$\begin{aligned}\rho((L-\mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) &< \ 2\left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}}\right)^n \cdot e^{-\pi\lambda_1(L)^2/4}\rho(L) \\ &<_{(1)} \ 3\left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}}\right)^n \cdot e^{-\pi\lambda_1(L)^2/4}\end{aligned} \tag{25}$$

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

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

$$\begin{aligned}
\frac{\rho((L-\mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n)}{\rho_d(\mathbf{y}')} &< 3e^{n\ln\left(\frac{\lambda_1(L)\sqrt{\pi e}}{\sqrt{2n}}\right) - \pi\lambda_1(L)^2/4 + \pi\|\mathbf{y}'\|^2/d^2} \\
&< 3e^{n\ln(\lambda_1(L)/\sqrt{n}) - \pi\lambda_1(L)^2/4 + \pi\lambda_1(L)^2/9 + n\ln\sqrt{\pi e/2}} \\
&<_{(1)} 3e^{n\ln(3) - \frac{9}{4}n\pi + n\pi + n\ln\sqrt{\pi e/2}} \\
&= 3e^{n(\ln 3 - \frac{5}{4}\pi + \ln\sqrt{\pi e/2})},
\end{aligned} \tag{26}$$

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

$$g(x) := \ln(x) - 5\pi x^2/36 + \ln(\sqrt{\pi e/2}) \tag{27}$$

The derivative of g is

$$g'(x) = 1/x - 5\pi x/18 \tag{28}$$

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

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

$$\rho((L-\mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n}\rho_d(L-\mathbf{y}). \tag{29}$$

□

Corollary 9. *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 $\lambda_1(L) > \frac{3b}{a}dist(\mathbf{y}, L)$ and $\lambda_1(L) > 3\sqrt{n}/a$, we have*

$$\rho_{\Sigma^{-1}}((L-\mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) \le \rho_{\frac{1}{a}}((L-\mathbf{y}) \setminus \frac{\lambda_1(L)}{2} \cdot B_2^n) < 2^{-n}\rho_{\frac{1}{b}}(L-\mathbf{y}) \le 2^{-n}\rho_{\Sigma^{-1}}(L-\mathbf{y}). \tag{30}$$

A.2 Smoothing of Gaussian with a phase

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

Theorem 10. *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

$$\begin{aligned}
Y(\mathbf{x}) &= \sum_{\mathbf{y} \in L+\mathbf{u}} h(\mathbf{y}) \rho_s(\mathbf{x} - \mathbf{y}) \\
&= \sum_{\mathbf{y} \in L+\mathbf{u}} \exp\left(-\pi \left(\frac{\|\mathbf{y}\|^2}{r^2} + \frac{\|\mathbf{x} - \mathbf{y}\|^2}{s^2}\right)\right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle} \\
&= \exp\left(-\frac{\pi}{r^2 + s^2} \|\mathbf{x}\|^2\right) \sum_{\mathbf{y} \in L+\mathbf{u}} \exp\left(-\pi \left(\frac{t}{rs}\right)^2 \cdot \|\mathbf{y} - \frac{r^2}{t^2}\mathbf{x}\|^2\right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle} \\
&= \rho_t(\mathbf{x}) \cdot \sum_{\mathbf{y} \in L+\mathbf{u}} \exp\left(-\pi \left(\frac{t}{rs}\right)^2 \cdot \|\mathbf{y} - \frac{r^2}{t^2}\mathbf{x}\|^2\right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle}
\end{aligned} \tag{31}$$

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

$$\begin{aligned}
&\sum_{\mathbf{y} \in L+\mathbf{u}} \exp\left(-\pi \left(\frac{t}{rs}\right)^2 \cdot \|\mathbf{y} - \frac{r^2}{t^2}\mathbf{x}\|^2\right) \cdot e^{2\pi i \cdot \langle \mathbf{y}, \mathbf{z} \rangle} \\
=& \sum_{\mathbf{y} \in L} \rho_{\frac{rs}{t}}\left(\mathbf{y} + \mathbf{u} - \frac{r^2}{t^2}\mathbf{x}\right) \cdot e^{2\pi i \cdot \langle \mathbf{y} + \mathbf{u}, \mathbf{z} \rangle} \\
=& \sum_{\mathbf{y} \in L} g(\mathbf{y} + \mathbf{u} - \frac{r^2}{t^2}\mathbf{x}) \cdot e^{2\pi i \cdot \left\langle \frac{r^2}{t^2}\mathbf{x}, \mathbf{z} \right\rangle} \\
=_{(1)}& \sum_{\mathbf{w} \in L^*} \hat{g}(\mathbf{w}) \cdot e^{2\pi i \cdot \left\langle \mathbf{u} - (r/t)^2 \mathbf{x}, \mathbf{w} \right\rangle} \cdot e^{2\pi i \cdot \left\langle \frac{r^2}{t^2}\mathbf{x}, \mathbf{z} \right\rangle} \\
=& \sum_{\mathbf{w} \in L^*} \rho_{t/rs}(\mathbf{w} - \mathbf{z}) \cdot e^{2\pi i \cdot \left(\langle \mathbf{u}, \mathbf{w} \rangle - \left\langle (r/t)^2 \mathbf{x}, \mathbf{w} - \mathbf{z} \right\rangle \right)}
\end{aligned} \tag{32}$$

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

Applying Lemma 7 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 $t = \sqrt{r^2 + s^2}$. $dist(\mathbf{y}, L)$ in Lemma 7 satisfies

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

Back to Eqn. (32), 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

$$\sum_{\mathbf{w}\in L^*} \rho_{t/rs}(\mathbf{w}-\mathbf{z}) \cdot e^{2\pi i\cdot\left(\langle \mathbf{u},\mathbf{w}\rangle - \left\langle (r/t)^2\mathbf{x},\mathbf{w}-\mathbf{z}\right\rangle\right)} \approx \rho_{t/rs}(\mathbf{z}') \cdot e^{2\pi i\cdot\left(\langle \mathbf{u},\kappa_{L^*}(\mathbf{z})\rangle + \left\langle (r/t)^2\mathbf{x},\mathbf{z}'\right\rangle\right)} \tag{33}$$

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 11. *For any $\mathbf{x}\in\mathbb{R}^n$ such that $\|\mathbf{x}\|>0$. Suppose the amplitude of $\mathbf{v}\in\mathbb{R}^n$ is $f(\mathbf{v}) = \rho_r(\mathbf{v})\cdot e^{2\pi i(\langle \mathbf{v},\mathbf{y}\rangle + w)}$ 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*

$$g(u) = \lambda\cdot\rho_{\|\mathbf{x}\|\cdot r}(u)\cdot e^{2\pi i\cdot u\cdot\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}}. \tag{34}$$

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

$$f(\mathbf{v}) = \rho_r(\mathbf{v})\cdot e^{2\pi i\langle \mathbf{v}+\mathbf{v}',\mathbf{y}\rangle} \tag{35}$$

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 $x_j\neq 0$,

$$g_j(u_j) = \rho_{x_j\cdot r}(u_j)\cdot e^{2\pi i\cdot(u_j\cdot y_j/x_j) + v_j'\cdot y_j} \tag{36}$$

Then the Fourier transform of g_j is

$$\hat{g}_j(z) = \begin{cases} e^{2\pi i\cdot v_j'\cdot y_j} & \text{when } x_j = 0; \\ e^{-\pi r^2(x_i\cdot z - y_i)^2}\cdot e^{2\pi i\cdot v_j'\cdot y_j} & \text{when } x_j\neq 0; \end{cases} \tag{37}$$

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

$$\hat{g}(z) := \prod_{j=1}^{n}\hat{g}_j(z) = e^{-\pi r^2(\|\mathbf{x}\|^2\cdot z^2 - 2\langle \mathbf{x},\mathbf{y}\rangle\cdot z + \delta)}\cdot e^{2\pi i\cdot w} = e^{-\pi r^2\|\mathbf{x}\|^2\cdot(z-\theta)^2 + \delta'}\cdot e^{2\pi i\cdot w} \tag{38}$$

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

$$g(u) = \hat{\hat{g}}(u) = \lambda\cdot\rho_{\|\mathbf{x}\|\cdot r}(u)\cdot e^{2\pi i\cdot u\cdot\theta}. \tag{39}$$

where λ is some fixed complex number. □