Quantum Algorithms for Lattice Problems

Yilei Chen*

April 10, 2024

Abstract

We show a polynomial time quantum algorithm for solving the learning with errors problem (LWE) with certain polynomial modulus-noise ratios. Combining with the reductions from lattice problems to LWE shown by Regev [J.ACM 2009], we obtain polynomial time quantum algorithms for solving the decisional shortest vector problem (GapSVP) and the shortest independent vector problem (SIVP) for all n-dimensional lattices within approximation factors of $\tilde{\Omega}(n^{4.5})$. Previously, no polynomial or even subexponential time quantum algorithms were known for solving GapSVP or SIVP for all lattices within any polynomial approximation factors.

To develop a quantum algorithm for solving LWE, we mainly introduce two new techniques. First, we introduce Gaussian functions with *complex* variances in the design of quantum algorithms. In particular, we exploit the feature of the *Karst wave* in the discrete Fourier transform of complex Gaussian functions. Second, we use *windowed* quantum Fourier transform with complex Gaussian windows, which allows us to combine the information from both time and frequency domains. Using those techniques, we first convert the LWE instance into quantum states with purely imaginary Gaussian amplitudes, then convert purely imaginary Gaussian states into classical linear equations over the LWE secret and error terms, and finally solve the linear system of equations using Gaussian elimination. This gives a polynomial time quantum algorithm for solving LWE.

*IIIS, Tsinghua University, Shanghai Artificial Intelligence Laboratory, and Shanghai Qi Zhi Institute. Emails: chenyilei@mail.tsinghua.edu.cn. chenyilei.ra@gmail.com. Supported by Tsinghua University startup funding.

Contents

1 Introduction

An n-dimensional lattice L is a discrete additive subgroup of $\mathbb{R}^n$. Given n linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{R}^n\}$, the lattice generated by $\mathbf{B}$ is

$$L(\mathbf{B}) = L(\mathbf{b}_1, ..., \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \cdot \mathbf{b}_i, x_i \in \mathbb{Z} \right\}.$$

In this article we measure the length of a vector in the ℓ_2 norm by default. The minimum distance $\lambda_1(L)$ of a lattice L is the length of its shortest non-zero vector: $\lambda_1(L) = \min_{\mathbf{x} \in L \setminus \{\mathbf{0}\}} \|\mathbf{x}\|$. The i^{th} successive minimum $\lambda_i(L)$ is the smallest number r such that L contains i linearly independent vectors of norm at most r.

The shortest vector problem (SVP) asks to find a lattice vector of length λ_1. More generally, let $\gamma(n) \geq 1$ be an approximation factor, we consider the approximation version of SVP and its close variants.

Definition 1.1 (Approximate SVP)**.** *Given a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* L*, the* SVP_γ *problem asks to output a non-zero lattice vector* $\mathbf{Bx}$*,* $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$*, such that* $\|\mathbf{Bx}\| \leq \gamma(n) \cdot \lambda_1(L)$*.*

Definition 1.2 (GapSVP)**.** *Given a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* L *and a number* $d > 0$*, the* GapSVP_γ *problem asks to decide whether* $\lambda_1(L) \leq d$ *or* $\lambda_1(L) > d \cdot \gamma(n)$*.*

Definition 1.3 (Shortest independent vector problem (SIVP))**.** *Given a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* L*, the* SIVP_γ *problem asks to output a set of* n *linearly independent vectors of length at most* $\gamma(n) \cdot \lambda_n(L)$*.*

The celebrated LLL algorithm [LLL82] solves SVP with $2^{O(n)}$ approximation in poly(n) time. The approximation factor achieved by polynomial time algorithms has been reduced to $\exp\left(O\left(\frac{n \log\log n}{\log n}\right)\right)$, which is slightly subexponential [Sch87, AKS01]. For the problem of finding the exact shortest non-zero vector, algorithms have been improved over the years [Kan87, AKS01, NV08, MV13, ADRS15] and the best running time is in $2^{O(n)}$. A trade-off between the running time and the approximation factor is given by Schnorr [Sch87], giving roughly $2^{\tilde{O}(n^c)}$ time algorithms for solving SVP with $2^{\tilde{O}(n^{1-c})}$ approximation, for $c \in (0, 1)$. Those are the best asymptotic parameters (without concerning the constant multiplicative factors in the exponent) for SVP_γ and GapSVP_γ achieved to date for both classical and quantum algorithms for general lattices.

Even though the best polynomial time algorithms for SVP achieve only exponential approximation factors, the capability of finding short vectors of lattices has led to breakthroughs in computation and number theory, given algorithms for factoring polynomials over $\mathbb{Q}$ and diophantine approximation [LLL82], integer programming [Len83], solving the low-density subset sum problem [Bri84, LO85], giving approximate solutions for the closest vector problem [Bab86], the first disproof of the Mertens conjecture [OtR85], and solving various problems in cryptography, e.g., [Sha82, Cop97, NS99].

Lattice and LWE. In the literature, solving short vector problems with polynomial approximation factors for *all* lattices has been classically reduced to the short integer solution (SIS) problem by Ajtai [Ajt96], and quantumly reduced to the dihedral coset problem (DCP, with some caveats) and the learning with errors problem (LWE) by Regev [Reg04, Reg09]. In this article we focus on the LWE problem, which essentially asks to learn a secret vector given many noisy linear samples.

Definition 1.4 (Learning with errors (LWE) [Reg09]). *Let n, m, q be positive integers. Let $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector where each entry is sampled from some distribution $DistS$. The search LWE problem $\mathsf{LWE}_{n,m,q,DistS,DistE}$ asks to find the secret $\mathbf{s}$ given access to an oracle that outputs $\mathbf{a}_i$, $\langle \mathbf{s}, \mathbf{a}_i \rangle + e_i \pmod q$ on its i^{th} query, for $i = 1, ..., m$. Here each $\mathbf{a}_i$ is a uniformly random vector in $\mathbb{Z}_q^n$, and each error term e_i is sampled from $DistE$ over $\mathbb{Z}_q$.*

The decisional LWE problem $\mathsf{DLWE}_{n,m,q,DistS,DistE}$ asks to distinguish whether we are given samples $(\mathbf{A}, \mathbf{y}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ from the LWE distribution, i.e., $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n \times m})$, $\mathbf{y} = \mathbf{A}^T \mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m$ where $\mathbf{s} \leftarrow DistS^n$, $\mathbf{e} \leftarrow DistE^m$; or from the uniformly random distribution over $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$.

Typically, the secret is sampled from the uniform random distribution over $\mathbb{Z}_q^n$, the error is sampled from the discrete Gaussian distribution over $\mathbb{Z}$ with standard deviation $\alpha q / \sqrt{2\pi}$ for some $\alpha \in (0, 1)$, denoted by $D_{\mathbb{Z}, \alpha q}$. The search and decisional LWE problems are proven to be equivalent for polynomially large prime moduli [Reg09] and polynomially-smooth moduli [MM11, MP12].

Regev [Reg09] and Peikert, Regev, Stephens-Davidowitz [PRS17] show that to construct an efficient quantum algorithm for approximate SVP for all lattices, it suffices to construct an efficient quantum algorithm for solving the search or decisional version of LWE.

Lemma 1.5 ([Reg09], [PRS17]). *Let $n, m, q \in \mathbb{N}^+$, $\alpha \in (0, 1)$ satisfy $m \geq \Omega(n \log q)$, $\alpha q \geq 2\sqrt{n}$. If there is a $\mathrm{poly}(n)$ time algorithm that solves $\mathsf{LWE}_{n,m,q,U(\mathbb{Z}_q),D_{\mathbb{Z},\alpha q}}$ or $\mathsf{DLWE}_{n,m,q,U(\mathbb{Z}_q),D_{\mathbb{Z},\alpha q}}$, then there is a $\mathrm{poly}(n)$ time quantum algorithm that solves SIVP_γ and GapSVP_γ for all lattices for $\gamma \in \tilde{O}(n/\alpha)$.*

However, no efficient classical or quantum algorithms have been proposed for solving LWE.

Hard lattice problems (in particular, LWE) are extremely useful in building advanced encryption schemes such as fully homomorphic encryptions for classical [Gen09, BV11] and quantum computations [Mah18]. LWE and lattice problems in general (e.g. [HPS98, Reg09]) are also popular candidates for the NIST post-quantum cryptography standardization due to their conjectured hardness against quantum computers. Part of the reasons behind the conjectured quantum hardness of lattice problems is: the existing quantum techniques with (sub)exponential advantages, such as period finding [Sim97, Sho99], quantum walk [CCD+03], Kuperberg's sieve [Kup05], and others (see more in `https://quantumalgorithmzoo.org/`), do not seem to help in creating quantum algorithms for SVP for *general* lattices with super-polynomial speedups.

Let us remark that efficient quantum algorithms for finding short vectors for *special* lattices used in number theory have been proposed in [EHKS14, BS16, CDPR16]. Recently a quantum filtering technique was proposed for solving certain *variants* of SIS and LWE [CLZ22] where no classical algorithm is known. However, those variants are not known to be as hard as solving approximate SVP for *all* lattices. Overall, those quantum algorithms show interesting ideas of tackling (variants of) lattice problems from different angles. Nevertheless, showing a polynomial (or even subexponential) time quantum algorithm for SVP with *polynomial* approximation factors for *all* lattices remains widely open, and seems to require dramatically new ideas.

1.1 Main results

We provide a polynomial time quantum algorithm for solving LWE with certain polynomial modulus-noise ratio.

Theorem 1.6 (Theorem 3.1)**.** *Let $n, m, q \in \mathbb{N}$, $\alpha \in (0,1)$ be such that $m \geq \Omega(n \log q)$, $q \in \tilde{\Omega}((\alpha q)^4 m^2)$. There is a quantum algorithm that solves $\mathsf{LWE}_{n,m,q,U(\mathbb{Z}_q),D_{\mathbb{Z},\alpha q}}$ in time $\mathrm{poly}(m, \log q, \alpha q)$.*

To get the best approximation factor for solving worst-case lattice problems, we set $q \in \tilde{O}(n^4)$, $m \in \Omega(n \log q)$, $\alpha \in \tilde{O}(n^{-3.5})$. Then, as a corollary of Theorem 1.6 and Lemma 1.5:

Corollary 1.7. *There exist $\mathrm{poly}(n)$ time quantum algorithms that solve SIVP_γ and GapSVP_γ for all n-dimensional lattices for $\gamma \in \tilde{O}(n^{4.5})$.*

Let us remark that the modulus-noise ratio achieved by our quantum algorithm is still too large to break the public-key encryption schemes based on (Ring)LWE used in practice. In particular, we have not broken the NIST PQC standardization candidates. For example, for CRYSTALS-Kyber [BDK+18], the error term is chosen from a small constant range, the modulus is $q = 3329$, the dimension is $n = 256 \cdot k$ where $k \in \{3, 4, 5\}$, so we can think of q as being almost linear in n. For our algorithm, if we set $\alpha q \in O(1)$, then our algorithm applies when $q \in \tilde{\Omega}(n^2)$, so we are not able to break CRYSTALS-Kyber yet. We leave the task of improving the approximation factor of our quantum algorithm to future work.

1.2 Main techniques: Gaussian functions with complex variances

Our algorithm uses Gaussian functions with complex variances. Let $a, b \in \mathbb{R}$ such that $a > 0$, the complex Gaussian function and its Fourier transform are [Smi11]:

$$g(x) = \exp\left(-\pi \frac{x^2}{a+bi}\right) = \exp\left(-\pi \frac{(a-bi)x^2}{a^2+b^2}\right), \quad \hat{g}(y) = \sqrt{a+bi} \cdot \exp\left(-\pi(a+bi)y^2\right). \tag{1}$$

Complex Gaussian function has been used in other areas in mathematics and engineering, as diverse as analytic number theory [Tit51] and signal analysis [Pap77]. In signal analysis, it is an example of "sophisticated signals", which refers to signals where the product of time and frequency duration can be infinitely large [Pap77, P.275]. Indeed, here the width of g is roughly $\sqrt{\frac{a^2+b^2}{a}}$, the width of $\hat{g}$ is roughly $\sqrt{\frac{1}{a}}$, so their product tends to infinity when $|b|$ goes to infinity. There are other interesting properties and applications of complex Gaussians. However, to the best of our knowledge, we are not aware of any previous use of complex Gaussian in designing quantum algorithms.

Let $r, s > 0$, let $f_{r,s}(x) := \exp\left(-\pi\left(\frac{1}{r^2} + \frac{i}{s^2}\right)x^2\right)$. Intuitively, when $s \gg r$, $f_{r,s}$ is close to the Gaussian function with real variance; when s gets smaller, the continuous Fourier transform of $f_{r,s}$ gets wider. We will crucially use three features of complex Gaussians. First, we can efficiently create a quantum state with complex Gaussian amplitude $|\phi\rangle := \sum_{x \in \mathbb{Z}_P} f_{r,s}(x) |x\rangle$, where $P \geq r\sqrt{n}$. To create $|\phi\rangle$, we first create a Gaussian state $\sum_{x \in \mathbb{Z}_P} \exp\left(-\pi \frac{x^2}{r^2}\right)|x\rangle$ by the well-known algorithm of Grover and Rudolph [GR02], then use the phase kickback trick [CEMM98] to insert the phase term as follows:

$$\sum_{x \in \mathbb{Z}_P} e^{-\pi \frac{x^2}{r^2}} |x\rangle \mapsto \sum_{x \in \mathbb{Z}_P} e^{-\pi \frac{x^2}{r^2}} |x\rangle \left|\frac{x^2}{s^2}\right\rangle \mapsto \sum_{x \in \mathbb{Z}_P} e^{-\pi \frac{x^2}{r^2}} e^{-\pi i \frac{x^2}{s^2}} |x\rangle \left|\frac{x^2}{s^2}\right\rangle \mapsto \sum_{x \in \mathbb{Z}_P} e^{-\pi\left(\frac{1}{r^2} + \frac{i}{s^2}\right)x^2} |x\rangle = |\phi\rangle.$$

The second feature is that the *center* and *phase* of a complex Gaussian can be switched to each other, denoted as "*center* = *phase*". This is most easily seen from the purely imaginary Gaussian, namely, for

$$f_{\infty,s}(x) = e^{-\pi i \frac{(x-c)^2}{s^2}} = e^{-\pi i \frac{x^2}{s^2}} e^{2\pi i \frac{cx}{s^2}} e^{-\pi i \frac{c^2}{s^2}}, \tag{2}$$

the LHS views c as the center, and the RHS views c as a factor in the phase $e^{2\pi i\frac{cx}{s^2}}$. Such a feature is useful when we use Fourier transform to connect information from time domain and the Fourier domain.

The third feature (the most important one) called *Karst wave* appears in the DFT of complex Gaussians. Suppose we start with a quantum state $\sum_{x\in\mathbb{Z}_P} f_{r,s}(x)\,|x\rangle$ and apply quantum Fourier transform over $\mathbb{Z}_P$ on it. We get

$$|\psi\rangle := \sum_{y\in\mathbb{Z}_P}\sum_{x\in\mathbb{Z}_P} f_{r,s}(x)e^{-2\pi i\frac{xy}{P}}\,|y\rangle =_{(a)} \sum_{y\in\mathbb{Z}_P}\sum_{z\in P\cdot\mathbb{Z}} \exp\left(-\pi\frac{r^2s^2(s^2-r^2i)}{P^2(s^4+r^4)}(y+z)^2\right)|y\rangle\,,$$

where (a) uses the Poisson summation formula (PSF, Lemma 2.4). The real Gaussian width is around $\frac{Pr}{s^2}$, so when $r > s^2$, the width is even larger than P. Therefore, the amplitude of $|\psi\rangle$ looks chaotic in general. However, when $\frac{s^2r^4}{2(s^4+r^4)} \in 2\mathbb{Z}$ (when $r \geq s^2$, this roughly means s^2 is very close to $4\mathbb{Z}$), we can show that y concentrates on some numbers near $\frac{P}{s^2}\mathbb{Z}$. The proof is as follows: for any $y \in \mathbb{Z}_P$, the amplitude of $|y\rangle$ in $|\psi\rangle$ is proportional to

$$\begin{aligned}
&\sum_{z\in P\cdot\mathbb{Z}} \exp\left(-\pi\frac{r^2s^2(s^2-r^2i)}{P^2(s^4+r^4)}(y+z)^2\right)\\
=\;&\sum_{z\in P\cdot\mathbb{Z}} \exp\left(-\pi\frac{r^2s^4}{P^2(s^4+r^4)}(y+z)^2\right)\exp\left(\pi i\frac{r^4s^2}{P^2(s^4+r^4)}(y+z)^2\right)\\
=_{(a)}\;&\sum_{z\in P\cdot\mathbb{Z}} \exp\left(-\pi\frac{r^2s^4}{P^2(s^4+r^4)}(y+z)^2\right)\exp\left(\pi i\frac{r^4s^2}{P^2(s^4+r^4)}\left(y^2+2yz\right)\right)\\
=_{PSF}\;&\sum_{z'\in\mathbb{Z}/P} \exp\left(-\pi\frac{P^2(s^4+r^4)}{r^2s^4}\left(z'-\frac{r^4s^2}{P^2(s^4+r^4)}y\right)^2\right)\cdot e^{\pi i\frac{r^4s^2}{P^2(s^4+r^4)}y^2}\cdot e^{2\pi i\left\langle y,z'-\frac{r^4s^2}{P^2(s^4+r^4)}y\right\rangle}\\
=\;&\sum_{z'\in\mathbb{Z}} \exp\left(-\pi\frac{s^4+r^4}{r^2s^4}\left(z'-\frac{r^4s^2}{P(s^4+r^4)}y\right)^2\right)\cdot e^{\pi i\frac{r^4s^2}{P^2(s^4+r^4)}y^2}\cdot e^{2\pi i\left\langle y,\frac{z'}{P}-\frac{r^4s^2}{P^2(s^4+r^4)}y\right\rangle}
\end{aligned}$$

where (a) uses $\frac{s^2r^4}{2(s^4+r^4)} \in 2\mathbb{Z}$ so that we can erase the z^2 term in the phase since $z \in P\mathbb{Z}$. Therefore y distributes as Gaussians centered around $\frac{P(s^4+r^4)}{r^4s^2}\mathbb{Z} \approx \frac{P}{s^2}\mathbb{Z}$ of width $\frac{s^2r}{\sqrt{s^4+r^4}}\cdot\frac{P(s^4+r^4)}{r^4s^2} \approx \frac{P}{r}$. We name this feature *Karst wave* because the sharp curve looks like Karst landscapes. See Figure 1 (bottom right) for an illustration.

Looking ahead, the Gaussian function with complex variance is intuitively useful for designing quantum algorithms for lattice problems since it has sharp tails in the time domain (like the Gaussian function with real variance, which has been used in the analysis of lattice problems since [MR07, Reg09]), and it has the interesting feature of Karst wave in the frequency domain (where we can accurately produce periodic patterns). However, even given the feature of Karst wave, it is still unclear how to use complex Gaussian to solve the LWE problem right away. To make use of complex Gaussians, we need another tool called *QFT with windows*.

Quantum Fourier transforms with windows. Let $Q \in \mathbb{N}$ be a modulus. Given some quantum state, say $|\phi\rangle := \sum_{x\in\mathbb{Z}_Q} g(x)\,|x\rangle$, and some "window" state $\sum_{y\in\mathbb{Z}_Q} w(y)\,|y\rangle$ that can be created efficiently

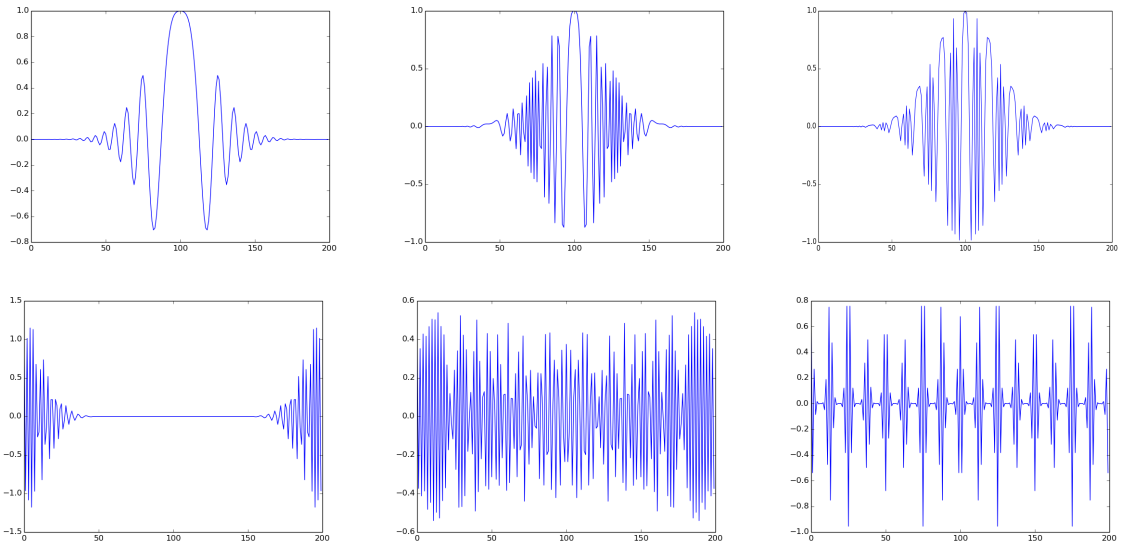

Figure 1: The real parts of $f_{r,s}(x-100)$ (up) and their DFTs over $\mathbb{Z}_P$ (bottom), where $P = 200$, $r = 54$, $s = 18$ (left), 7.5 (middle), 4.0001 (right). The DFTs are narrow (left), wide & chaotic (middle), wide & like the Karst wave (right). When $s = 4.0001$, $\frac{s^2r^4}{2(s^4+r^4)} \approx 8.00015 \approx 2\mathbb{Z}$, the weight of the DFT of $f_{r,s}$ concentrates around $\frac{200}{16}\mathbb{Z}$.

(think of $w(y)$ as a function with bounded domain, say $w(y) = \exp\left(-\pi\frac{y^2}{r^2}\right)$ for $|y| < r\sqrt{n} < \frac{Q}{2}$). Consider the following sequence of operations: first apply the operation

$$\sum_{x\in\mathbb{Z}_Q} g(x)\,|x\rangle \otimes \sum_{y\in\mathbb{Z}_Q} w(y)\,|y\rangle \mapsto \sum_{x\in\mathbb{Z}_Q} g(x)\,|x\rangle \otimes \sum_{y\in\mathbb{Z}_Q} w(y)\,|x+y \bmod Q\rangle\,,$$

then measure the last register and denote the result as $y' = x + y \bmod Q$. Then the residual state is $|\varphi\rangle := \sum_{x\in\mathbb{Z}_Q} g(x)w(y'-x \bmod Q)\,|x\rangle$. We refer to the whole process that takes $|\phi\rangle$ to $(|\varphi\rangle,\, y')$ as "applying a window on $|\phi\rangle$". Typically the window is applied before or after a QFT operation, so as to extract and combine the information from both the time domain and the Fourier domain. For example, suppose $|\phi\rangle$ is in the time domain, then we can think of y' as a piece of information extracted from the time domain, and $|\varphi\rangle$ is the residual state determined by y'. Then if we apply QFT on $|\varphi\rangle$ and measure it, we get information in the frequency domain.

For general g and w, the information from the time and frequency domain is not clearly related. But if g and w are carefully chosen, then the information in the time and frequency domains can be combined together in a useful way. The quantum wavelet transform [FW98], quantum curvelet transform [Liu09] in the literature can be viewed as special cases of using QFT with windows, where the windows are designed carefully for special purposes. For example, in the quantum curvelet transform proposed by Liu [Liu09], the window is designed specifically so that combing the information from both the time domain and the frequency domain leads to a precise estimation of the center of the input state $|\phi\rangle$.

In our quantum algorithm for solving lattice problems, we use QFT with complex Gaussian windows, where the parameters in the complex Gaussian windows are tuned carefully so that combining the

information from both the time domain and the frequency domain allows us to extract the higher order bits on the "peaks" of Karst waves, which contain information about lattice points.

1.3 Overview of our algorithm for solving LWE

Here is a high level overview of our quantum algorithm for solving LWE. In fact, the entire quantum algorithm we use just consists of QFTs, complex Gaussian windows, and other standard quantum computation tools. However, how to combine them together is highly non-trivial, the detail calculations are very complicated. So here we will only mention the most important ideas. We will provide a more detailed overview in §3.4 after all parameters used in the algorithm are defined.

Our quantum algorithm runs a quantum subroutine consisting of nine steps for $O(n)$ times. Every time we run the quantum subroutine, we will obtain a classical linear equation with random coefficients and the unknown variables are the LWE secrets and error terms. After running the quantum subroutine for $O(n)$ times we will get a full rank system of linear equations and compute the LWE secret and error terms by Gaussian elimination.

Now let us explain a bit about the nine quantum steps. We use $|\varphi_i\rangle$ to denote the state obtained at the end of Step i. See Figure 2 for an example of the states obtained in each step. The first step of the quantum subroutine applies a complex Gaussian window on a state with uniform superposition over a lattice related to the LWE instance, obtains a classical string $\mathbf{y}'$ and a complex Gaussian state $|\varphi_1\rangle$:

$$|\varphi_1\rangle = \sum_{k\in\mathbb{Z}, k\mathbf{x}-\mathbf{y}\in(r\log n)\mathcal{B}_\infty^n} \exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)\|k\mathbf{x}-\mathbf{y}\|^2\right)|k\mathbf{x}-\mathbf{y}\rangle\,,$$

where $\mathbf{x}$ is the secret vector we want to learn (related to the LWE secret and error terms), $\mathbf{y}\in\mathbb{Z}^n$ is an unknown vector at this moment but its information is carried in $\mathbf{y}'$. The support of $|\varphi_1\rangle$ is on a line in the same direction with the secret vector $\mathbf{x}$ (see Figure 2-(a)).

Note that $|\varphi_1\rangle$ looks very similar to a sample in the extrapolated dihedral coset problem (EDCP) [BKSW18]. An instance of EDCP in general looks like

$$\sum_{k\in\mathbb{Z}_P} f(k)\,|k\rangle\,|k\mathbf{x}-\mathbf{y} \bmod P\rangle\,,$$

for some amplitude function f and modulus P. In our setting $|\varphi_1\rangle$ looks like an EDCP instance without the first coordinate $|k\rangle$ in a separated register, so it is not exactly an EDCP instance but is similar. Let us remark that previous attempts of transforming lattice problems into EDCP-like states typically result into EDCP states with unknown terms in the amplitude [CHL$^+$23], or with known amplitude but can only guarantee the correctness for very few amount of EDCP samples [Reg04, BKSW18], therefore sophisticated quantum algorithms for solving EDCP (such as Kuperberg's algorithm [Kup05]) won't apply there. Likewise, we don't expect to obtain an efficient quantum algorithm right away from $|\varphi_1\rangle$. We need to work harder to either make the amplitude nicer or learn one coordinate from $\mathbf{y}$ (the later may turn $|\varphi_1\rangle$ into an instance of EDCP with known amplitude).

The five steps from Steps 2 to 6 together make sure that the amplitude of $|\varphi_6\rangle$ in Step 6 is highly structural, consisting of small Gaussian balls. Steps 2 to 6 make heavy use of QFT with complex Gaussian windows and involve complicated calculations related to Fourier transforms – we take QFT,

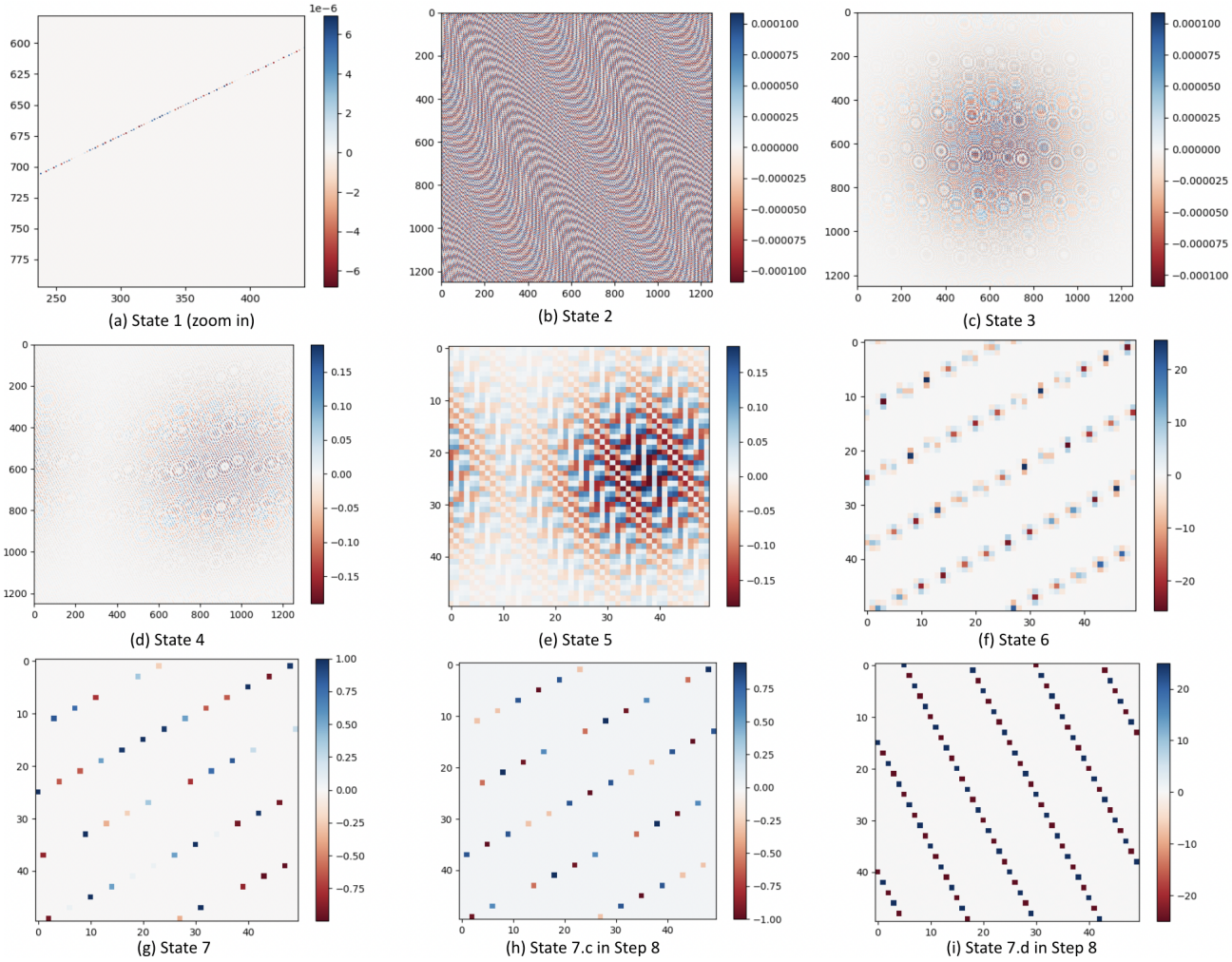

Figure 2: A proof-of-concept demonstration of the quantum states obtained in Steps 1 - 8. All pictures are depicting the real parts of the amplitudes of the states. The vertical (resp. horizontal) axis represents the first (resp. second) coordinate. Parameters (defined in §3.3) are set as $n = 2$, $D = 1$, $\mathbf{x} = D\mathbf{b} = (-1, 2)$, $u^2 = 5$, $t^2 = 4u^2 = 20$, $M = 2(t^2 + u^2) = 50$, $P = M^2/2 = 1250$, $r = 380.0$, $s^2 = 312.55$, $\sigma = 1.645$. We assume $\mathbf{z}' = (625, 625)$, $\mathbf{h}^* = (0, 0)$ for simplicity. The Python code for generating those figures is available at `https://github.com/wildstrawberry/ComplexGaussian`.

then apply a complex Gaussian window, then take QFT again, then make a partial measurement, then take QFT again to get $|\varphi_6\rangle$ in Step 6. If we think of $|\varphi_1\rangle$ as in the time domain, then $|\varphi_2\rangle, |\varphi_3\rangle, |\varphi_6\rangle$ are in the frequency domain, and they should in general look chaotic if we don't set the parameters carefully (from Figure 2-(b), (c), we see that $|\varphi_2\rangle$, $|\varphi_3\rangle$ indeed look chaotic). However, we tune the parameters carefully so that the amplitude of $|\varphi_6\rangle$ is highly structural due to the feature of Karst wave.

$|\varphi_6\rangle$ is an important state. From Figure 2-(f), we see that $|\varphi_6\rangle$ contains lines of Gaussian balls of small width σ, aligned in the direction of $\mathbf{x}$. We can then shift those Gaussian balls (using $\mathbf{y}'$, and other classical information obtained before Step 6) to make sure their centers are extractable. After extracting the centers of the Gaussian balls in $|\varphi_6\rangle$, we get $|\varphi_7\rangle$:

$$|\varphi_7\rangle = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} e^{2\pi i\frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{x} + \mathbf{v}' + \frac{M}{2}\mathbf{k} \bmod M\right\rangle, \tag{3}$$

where $\mathbf{v}'$ is an unknown vector, M is the modulus, D is some scaling parameter. As we can see from the expression of $|\varphi_7\rangle$ in Eqn. (3), and Figure 2-(g), now we get an EDCP-like state with purely *imaginary* Gaussian amplitudes, which is much easier to work with. We then use the nice property of imaginary Gaussian (i.e., *center* = *phase*) to obtain partial information of v_1' in Step 8 – we use the phase kickback trick to remove the quadratic term of j in the phase of $|\varphi_7\rangle$, see Figure 2-(h), and then take QFT to get a linear equation about v_1', see Figure 2-(i). We then obtain more information about $\mathbf{v}'$ using other tricks in Step 9, and finally get a linear equation about the LWE secret and error terms.

Organization. In the rest of the paper, we will first provide some background of lattice problems and quantum computation in §2, then provide the main quantum algorithm for solving LWE in §3, including a detailed overview of the algorithm and all proofs.

2 Preliminary

Notations and terminology. Let $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ be the set of complex numbers, real numbers, rational numbers, integers, and natural numbers (non-negative integers). Let $\mathbb{R}^+, \mathbb{N}^+$ denote positive reals and integers. Denote $\mathbb{Z}/q\mathbb{Z}$ by $\mathbb{Z}_q$. By default we represent the elements of $\mathbb{Z}_q$ by elements in $(-q/2, q/2]\cap\mathbb{Z}$. For $n \in \mathbb{N}$, let $[n] := \{1, ..., n\}$. The rounding operation $\lfloor a \rceil$ rounds a real number a to its nearest integer. For any integer $d \geq 2$, $\lfloor a \rceil_d$ rounds a real number a to its nearest integer in $d\mathbb{Z}$.

A vector in $\mathbb{R}^n$ (represented in column form by default) is written as a bold lower-case letter, e.g. $\mathbf{v}$. For a vector $\mathbf{v}$, the i^{th} component of $\mathbf{v}$ is denoted by v_i. The i^{th} to j^{th} components of $\mathbf{v}$ is denoted by $\mathbf{v}_{[i...j]}$. A matrix is written as a bold capital letter, e.g. $\mathbf{A}$. The i^{th} column vector of $\mathbf{A}$ is denoted by $\mathbf{a}_i$.

The length of a vector is the ℓ_p-norm $\|\mathbf{v}\|_p := (\sum v_i^p)^{1/p}$, or the infinity norm given by its largest entry $\|\mathbf{v}\|_\infty := \max_i\{|v_i|\}$. The ℓ_p norm of a matrix is the norm of its longest column: $\|\mathbf{A}\|_p := \max_i \|\mathbf{a}_i\|_p$. Let $\mathcal{B}_p^n$ (resp. $\bar{\mathcal{B}}_p^n$) denote the open (resp. closed) unit ball in $\mathbb{R}^n$ in the ℓ_p norm. By default we use ℓ_2-norm unless explicitly mentioned. Let $\mathbf{x} \in \mathbb{R}^n$, we have $\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\|_2 \leq \|\mathbf{x}\|_1$.

When a variable v is drawn uniformly random from the set S we denote as $v \leftarrow U(S)$. When a function f is applied on a set S, it means $f(S) := \sum_{x\in S} f(x)$.

In this paper, we use n as the default parameter to parameterize the computational complexity or the success probability of an algorithm. An algorithm is "efficient" if it runs in quantum polynomial time in n.

Definition 2.1 (Statistical distance)**.** *For two distributions over $\mathbb{R}^n$ with probability density functions f_1 and f_2, we define the statistical distance between them as*

$$D(f_1, f_2) = \frac{1}{2}\int_{\mathbb{R}^n} |f_1(\mathbf{x}) - f_2(\mathbf{x})| d\mathbf{x}.$$

When $D(f_1, f_2) \in \mathrm{negl}(n)$, we say f_1 and f_2 are statistically close, denoted as $f_1 \approx_s f_2$.

Lemma 2.2 (Hoeffding's inequality)**.** *If $X_1, ..., X_n$ are independent random variables such that $a_i \leq X_i \leq b_i$ for all i, then for the sum of those random variables $S_n := X_1 + ... + X_n$,*

$$\Pr[|S_n - \mathbb{E}[S_n]| \geq t] \leq 2\exp\left(-\frac{2t^2}{\sum_{i\in[n]}(b_i - a_i)^2}\right).$$

Fourier transform. The Fourier transform of a function $h : \mathbb{R}^n \to \mathbb{C}$ is defined to be

$$\hat{h}(\mathbf{w}) = \int_{\mathbb{R}^n} h(\mathbf{x}) \exp(-2\pi i \langle \mathbf{x}, \mathbf{w}\rangle) d\mathbf{x}.$$

We recall some formulas about Fourier transform (see [Gra08, P.100, Proposition 2.2.11]). If h is defined by $h(\mathbf{x}) = g(\mathbf{x} + \mathbf{v})$ for some function $g : \mathbb{R}^n \to \mathbb{C}$ and vector $\mathbf{v} \in \mathbb{R}^n$, then

$$\hat{h}(\mathbf{w}) = \hat{g}(\mathbf{w}) \cdot \exp(2\pi i \langle \mathbf{v}, \mathbf{w}\rangle). \tag{4}$$

If h is defined by $h(\mathbf{x}) = g(\mathbf{x}) \exp(2\pi i \langle \mathbf{x}, \mathbf{v}\rangle)$ for some function $g : \mathbb{R}^n \to \mathbb{C}$ and vector $\mathbf{v} \in \mathbb{R}^n$, then

$$\hat{h}(\mathbf{w}) = \hat{g}(\mathbf{w} - \mathbf{v}). \tag{5}$$

As a corollary of Eqns. (4) and (5), if h is defined by $h(\mathbf{x}) = f(\mathbf{x} + \mathbf{v}) \exp(2\pi i \langle \mathbf{x}, \mathbf{z}\rangle)$ for some function $f : \mathbb{R}^n \to \mathbb{C}$ and vectors $\mathbf{v}, \mathbf{z} \in \mathbb{R}^n$, then we define $g(\mathbf{x}) := f(\mathbf{x} + \mathbf{v})$, so $h(\mathbf{x}) = g(\mathbf{x}) \exp(2\pi i \langle \mathbf{x}, \mathbf{z}\rangle)$. Therefore $\hat{g}(\mathbf{w}) = \hat{f}(\mathbf{w}) \cdot \exp(2\pi i \langle \mathbf{v}, \mathbf{w}\rangle)$, and

$$\hat{h}(\mathbf{w}) = \hat{g}(\mathbf{w} - \mathbf{z}) = \hat{f}(\mathbf{w} - \mathbf{z}) \cdot \exp(2\pi i \langle \mathbf{v}, \mathbf{w} - \mathbf{z}\rangle). \tag{6}$$

As a corollary of Eqn. (6), if h is defined by $h(\mathbf{x}) = f(\mathbf{x} + \mathbf{v}) \exp(2\pi i \langle \mathbf{x} + \mathbf{v}, \mathbf{z}\rangle)$ for some function $f : \mathbb{R}^n \to \mathbb{C}$ and vectors $\mathbf{v}, \mathbf{z} \in \mathbb{R}^n$, then

$$\hat{h}(\mathbf{w}) = \hat{f}(\mathbf{w} - \mathbf{z}) \cdot \exp(2\pi i \langle \mathbf{v}, \mathbf{w}\rangle). \tag{7}$$

Lemma 2.3 (Inversion formula for special matrices (Sherman–Morrison formula))**.** *Let $\mathbf{M} \in \mathbb{C}^{n\times n}$ be invertible, $\mathbf{u} \in \mathbb{C}^n$, then $\mathbf{M} + \mathbf{u}\mathbf{u}^T$ is invertible iff $1 + \mathbf{u}^T\mathbf{M}^{-1}\mathbf{u} \neq 0$. Furthermore,*

$$\left(\mathbf{M} + \mathbf{u}\mathbf{u}^T\right)^{-1} = \mathbf{M}^{-1} - \frac{\mathbf{M}^{-1}\mathbf{u}\mathbf{u}^T\mathbf{M}^{-1}}{1 + \mathbf{u}^T\mathbf{M}^{-1}\mathbf{u}}. \tag{8}$$

2.1 Lattices

An n-dimensional lattice L of rank $k \leq n$ is a discrete additive subgroup of $\mathbb{R}^n$. Given k linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_k \in \mathbb{R}^n\}$, the lattice generated by $\mathbf{B}$ is

$$L(\mathbf{B}) = L(\mathbf{b}_1, ..., \mathbf{b}_k) = \left\{ \sum_{i=1}^{k} x_i \cdot \mathbf{b}_i, x_i \in \mathbb{Z} \right\}.$$

By default we work with full-rank lattices unless explicitly mentioned.

The minimum distance $\lambda_1(L)$ of a lattice L is the length (in the ℓ_2 norm by default) of its shortest nonzero vector: $\lambda_1(L) = \min_{\mathbf{x} \in L \setminus \{\mathbf{0}\}} \|\mathbf{x}\|$. More generally, the i^{th} successive minimum $\lambda_i(L)$ is the smallest radius r such that L contains i linearly independent vectors of norm at most r. We use λ_1^p to denote the minimum distance in the ℓ_p norm.

The dual of a lattice $L \in \mathbb{R}^n$ is defined as

$$L^* := \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{y}, \mathbf{x} \rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in L\}.$$

If $\mathbf{B}$ is a basis of a full-rank lattice L, then $\mathbf{B}^{-T}$ is a basis of L^*.

The determinant of a full-rank lattice $L(\mathbf{B})$ is $\det(L(\mathbf{B})) = |\det(\mathbf{B})|$.

Lemma 2.4 (Poisson Summation Formula)**.** *For any full-rank lattice L and any Schwartz function $f : \mathbb{R}^n \to \mathbb{C}$, we have $f(L) = \det(L^*)\hat{f}(L^*)$.*

Gaussians and lattices. For any $s > 0$, define the Gaussian function on $\mathbb{R}^n$ with width parameter s as follows (following the convention in [MR07]):

$$\forall \mathbf{x} \in \mathbb{R}^n, \ \rho_s(\mathbf{x}) = e^{-\pi \|\mathbf{x}\|^2 / s^2}. \tag{9}$$

For any $\mathbf{c} \in \mathbb{R}^n$, define $\rho_{s,\mathbf{c}}(\mathbf{x}) := \rho_s(\mathbf{x} - \mathbf{c})$. The subscripts s and $\mathbf{c}$ are taken to be 1 and $\mathbf{0}$ (respectively) when omitted. Note that although we call s the width of ρ_s, the actual standard deviation of ρ_s is $s/\sqrt{2\pi}$. The Fourier transform for Gaussian satisfies $\hat{\rho_s} = s^n \rho_{1/s}$. From Poisson summation formula we have $\rho_s(L) = s^n \cdot \det(L^*) \cdot \rho_{1/s}(L^*)$.

For any real $s > 0$, integer n, define the continuous Gaussian distribution D_s as:

$$\forall \mathbf{x} \in \mathbb{R}^n, \ D_s(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{s^n}.$$

For any $\mathbf{c} \in \mathbb{R}^n$, $s \in \mathbb{R}^+$, and lattice $L \subset \mathbb{R}^n$, define the discrete Gaussian distribution $D_{L+\mathbf{c},s}$ as:

$$\forall \mathbf{x} \in L + \mathbf{c}, \ D_{L+\mathbf{c},s}(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{\rho_s(L + \mathbf{c})}.$$

The following Gaussian tail bound over lattices is due to Banaszczyk.

Lemma 2.5 (Lemma 1.5 [Ban93])**.** *For any n-dimensional lattice L, and $r \geq \frac{1}{\sqrt{2\pi}}$, $\mathbf{c} \in \mathbb{R}^n$,*

$$\begin{aligned} \rho(L \setminus r\sqrt{n}\mathcal{B}^n) &< \left(r\sqrt{2\pi e} \cdot e^{-\pi r^2}\right)^n \rho(L), \\ \rho((L - \mathbf{c}) \setminus r\sqrt{n}\mathcal{B}^n) &< 2\left(r\sqrt{2\pi e} \cdot e^{-\pi r^2}\right)^n \rho(L). \end{aligned} \tag{10}$$

Lemma 2.6 (Lemma 2.10 [Ban95]). *For any n-dimensional lattice L, $\mathbf{c} \in \mathbb{R}^n$, $r > 0$, one has*

$$\rho((L - \mathbf{c}) \setminus r\mathcal{B}_\infty^n) < \left(2n \cdot e^{-\pi r^2}\right) \rho(L).$$

Claim 2.7 (Adapted from Claim 8.1 [RS17]). *For any $n \geq 1$, $s > 0$,*

$$s^n(1 + 2e^{-\pi s^2})^n \leq \rho_s(\mathbb{Z}^n) \leq s^n(1 + (2 + 1/s)e^{-\pi s^2})^n.$$

In particular, when $s \geq \log n$,

$$s^n \leq \rho_s(\mathbb{Z}^n) \leq 2s^n.$$

Smoothing parameter. We recall the definition of smoothing parameter for Gaussian over lattices and some useful facts.

Definition 2.8 (Smoothing parameter [MR07]). *For any lattice L and positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(L)$ is the smallest real $s > 0$ such that $\rho_{1/s}(L^* \setminus \{\mathbf{0}\}) \leq \epsilon$.*

For example, $\eta_{0.0864348}(\mathbb{Z}) \approx 1$.

We use [MR07, Lemma 4.2] which says when s is large enough, then the statistical properties of discrete Gaussians are very close to continuous Gaussians.

Lemma 2.9. *For any n-dimensional lattice L, point $\mathbf{c} \in \mathbb{R}^n$, unit vector $\mathbf{u}$, and $\epsilon \in (0, 1)$, $s \geq 2\eta_\epsilon(L)$,*

$$\begin{aligned} \left|\mathbb{E}_{\mathbf{x} \leftarrow D_{L,s,\mathbf{c}}} \left[\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle\right]\right| &\leq \frac{\epsilon s}{1 - \epsilon}, \\ \left|\mathbb{E}_{\mathbf{x} \leftarrow D_{L,s,\mathbf{c}}} \left[\langle \mathbf{x} - \mathbf{c}, \mathbf{u} \rangle^2\right] - \frac{s^2}{2\pi}\right| &\leq \frac{\epsilon s^2}{1 - \epsilon}. \end{aligned}$$

Other properties of smoothing parameters will be mentioned when needed.

q-ary lattices. Given $n < m \in \mathbb{N}$ and a modulus $q \geq 2$, for $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, define q-ary lattices as

$$\begin{aligned} L_q(\mathbf{A}) &= \left\{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}^n \text{ such that } \mathbf{x} \in \mathbf{A}^T \cdot \mathbf{s} + q\mathbb{Z}^m\right\}; \\ L_q^\perp(\mathbf{A}) &= \left\{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{x} \equiv \mathbf{0} \pmod q\right\}. \end{aligned} \tag{11}$$

Those two lattices are dual of each other up to a factor of q, i.e., $L_q(\mathbf{A}) = q \cdot L_q^\perp(\mathbf{A})^*$.

Lemma 2.10. *Let $q \geq 2, m \geq 2n \log_2 q$. Let $\mathcal{V} := \{\mathbf{v}_1, ..., \mathbf{v}_\ell\}$ be a set of ℓ distinct vectors in $\mathbb{Z}_q^m$. Then for all but at most $\ell \cdot q^{-0.16n}$ fraction of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we have*

$$\forall \mathbf{s} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}_n\}, \quad \forall \mathbf{v} \in \mathcal{V}, \quad \|\mathbf{A}^T\mathbf{s} + \mathbf{v} \bmod q\|_\infty \geq \frac{q}{4}.$$

Proof. The lemma is proven when q is a prime and $\mathcal{V} = \{\mathbf{0}_m\}$ in [GPV08, Lemma 5.3]. Here we extend the proof to a general q and a general set of vectors $\mathcal{V}$.

For any fixed non-zero $\mathbf{s} \in \mathbb{Z}_q^n$, wlog assuming s_1 is a non-zero entry of $\mathbf{s}$. Then for any $\mathbf{a} \in \mathbb{Z}_q^n$, for any $v \in \mathbb{Z}_q$, $y := \langle \mathbf{a}, \mathbf{s} \rangle + v \mod q$ can be written as $y = s_1 a_1 + w \mod q$ for some $w \in \mathbb{Z}_q$. We observe that for any $q \in \mathbb{N}^+$, for any $w \in \mathbb{Z}_q$, for any non-zero $s_1 \in \mathbb{Z}_q$,

$$\Pr_{a_1 \in \mathbb{Z}_q}[\, s_1 a_1 + w \bmod q \in (-q/4, q/4) \cap \mathbb{Z} \,] \leq 2/3,$$

here we represent $s_1 a_1 + w \bmod q$ by a number in $[-q/2, q/2) \cap \mathbb{Z}$; "$\leq 2/3$" holds since for any $z \in \mathbb{N}^+$, for any $w \in \mathbb{Z}$, $\ell \in \mathbb{Z}$, there can be at most z numbers in $\{w + k\ell \bmod (2z\ell)\}_{k \in \mathbb{Z}_{2z}}$ fitting in the set of $(-(2z\ell)/4, (2z\ell)/4) \cap \mathbb{Z}$, there can be at most $z+1$ numbers in $\{w + k\ell \bmod ((2z+1)\ell)\}_{k \in \mathbb{Z}_{2z+1}}$ fitting in the set of $(-(2z+1)\ell/4, (2z+1)\ell/4) \cap \mathbb{Z}$, and $2/3$ is the largest number in $\left\{ \frac{z+1}{2z+1} \mid z \in \mathbb{N}^+ \right\}$; the equality holds when $q \in 3^k \cdot \mathbb{N}$ for some $k \geq 1$, $s_1 \in (q/3) \cdot \mathbb{Z}/q\mathbb{Z}$, $s_1 \neq 0$, and for some $w \in \mathbb{Z}_q$ (for example, when $q = 15$, $s_1 = 5$, and $w = 2$).

Therefore, over the randomness of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, the probability that $\mathbf{A}^T \mathbf{s} + \mathbf{v} = \mathbf{y} \bmod q$ holds for some $\mathbf{y} \in \mathbb{Z}^m, \|\mathbf{y}\|_\infty < q/4$ is at most $(2/3)^m \leq (3/2)^{-2n \log_2 q} \leq q^{-1.16n}$. Applying a union bound over all $\mathbf{s} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}_n\}$ and all $\mathbf{v} \in \mathcal{V}$ completes the proof of Lemma 2.10. □

2.2 Quantum computation

We assume readers are familiar with basic concepts of quantum computation. All quantum backgrounds we need in this paper are available in standard textbooks of quantum computation, e.g., [NC16]. When writing a quantum state as $\sum_{x \in S} f(x) |x\rangle$, we typically omit the normalization factor except when needed.

The trace distance between two quantum states ρ and σ is defined as $D(\rho, \sigma) := \frac{1}{2} \operatorname{tr} |\rho - \sigma|$. Note that when ρ and σ commute they are diagonal in the same basis,

$$\rho = \sum_i r_i |i\rangle \langle i|, \quad \sigma = \sum_i s_i |i\rangle \langle i|,$$

for some orthonormal basis $|i\rangle$, then $D(\rho, \sigma) = \frac{1}{2} \operatorname{tr} |\sum_i (r_i - s_i) |i\rangle \langle i|| = \frac{1}{2} \sum_i |r_i - s_i|$.

The trace distance is preserved under unitary transformations, and is contractive under trace-preserving operations. When the trace distance of two states ρ and σ is negligible in n, we write $\rho \approx_t \sigma$.

When a state ρ can be approximately constructed within a negligible trace distance, we sometimes say the state is constructible without mentioning the negligible distance.

Lemma 2.11. *Let $|\phi\rangle$, $|\psi\rangle$ be un-normalized vectors s.t. $\| |\phi\rangle \| \geq \mu$ and $\| |\phi\rangle - |\psi\rangle \| \leq \delta$. Then*

$$D\left(\frac{1}{\| |\phi\rangle \|} |\phi\rangle, \frac{1}{\| |\psi\rangle \|} |\psi\rangle \right) = \sqrt{1 - \left(\frac{|\langle \phi | \psi \rangle|}{\| |\phi\rangle \| \| |\psi\rangle \|} \right)^2} \leq O\left(\sqrt{\frac{\delta}{\mu}} \right).$$

We use the following quantum algorithms:

Lemma 2.12 (Quantum Fourier Transform (QFT) [Kit95])**.** *Let $q \geq 2$ be an integer. The following unitary operator $\mathsf{QFT}_{\mathbb{Z}_q}$ can be implemented by $\operatorname{poly}(\log q)$ elementary quantum gates. When $\mathsf{QFT}_{\mathbb{Z}_q}$ is*

applied on a quantum state $|\phi\rangle := \sum_{x\in\mathbb{Z}_q} f(x)\,|x\rangle$*, we have*

$$\mathsf{QFT}_{\mathbb{Z}_q}\,|\phi\rangle = \sum_{y\in\mathbb{Z}_q}\sum_{x\in\mathbb{Z}_q}\frac{1}{\sqrt{q}}\cdot e^{-2\pi i\cdot xy/q}\cdot f(x)\,|y\rangle\,.$$

Lemma 2.13 (Phase kickback [CEMM98])**.** *Let* $M\in\mathbb{N}^+$*,* $f(x)\in\mathbb{Z}_M$*. If the transformation* $|x\rangle\mapsto|x\rangle\,|f(x)\rangle$ *is computable in time* T*, then the unitary transformation* $|x\rangle\mapsto e^{\frac{2\pi i f(x)}{M}}\,|x\rangle$ *can be performed in time* $\mathrm{poly}(T,\log(M))$*.*

It is well known that the Gaussian state $|\sigma_{n,R}\rangle := \sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n}\rho_R(\mathbf{y})\,|\mathbf{y}\rangle$ for some radius $R\le 2^{\mathrm{poly}(n)}$ can be prepared efficiently. Given Lemma 2.5, there is a $2^{-\Omega(n)}$ mass in the tail of $\rho_R(\mathbf{y})$ outside $R\sqrt{n}\mathcal{B}_2^n$, so we can prepare $|\sigma_{n,R}\rangle$ by generating n independent samples of one-dimensional Gaussian state $\left|\sigma_{1,R\sqrt{n}}\right\rangle$, which can be done efficiently within trace distance $2^{-\Omega(n)}$ [GR02]. Similarly, we can efficiently prepare $\left|\sigma^{\infty}_{n,R}\right\rangle := \sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\log n\mathcal{B}_\infty^n}\rho_R(\mathbf{y})\,|\mathbf{y}\rangle$ by generating n independent samples of one-dimensional Gaussian state $|\sigma_{1,R\log n}\rangle$. The discussion above is summarized in the following lemma.

Lemma 2.14 (Gaussian state preparation)**.** *Let* $n\in\mathbb{N}$*,* $R\in\mathbb{R}$ *satisfy* $1\le R\le 2^{n^c}$ *for some constant* $c\ge 0$*. Then the Gaussian states with* $\mathcal{B}_2^n$ *and* $\mathcal{B}_\infty^n$ *boundaries,* $|\sigma_{n,R}\rangle$ *and* $\left|\sigma^{\infty}_{n,R}\right\rangle$*, can both be prepared in* $\mathrm{poly}(n)$ *time within trace distance* $2^{-\Omega(n)}$*.*

In this paper we are interested in preparing complex Gaussian states.

Lemma 2.15 (Complex Gaussian state preparation)**.** *Let* $n\in\mathbb{N}$*,* $R\in\mathbb{R}$ *satisfy* $1\le R\le 2^{n^c}$ *for some constant* $c\ge 0$*. Let* $S>0$ *be a number such that* $\frac{1}{S^2}$ *can be efficiently computed within* $\frac{2^{-\Omega(n)}}{R^2n}$ *precision, i.e., we can compute* $\frac{1}{\tilde{S}^2}\in\frac{1}{S^2}\pm\frac{2^{-\Omega(n)}}{R^2n}$ *and* $\frac{1}{\tilde{S}^2}$ *is a rational number that can be represented by* $\mathrm{poly}(n)$ *bits. Then the complex Gaussian states with* $\mathcal{B}_2^n$ *and* $\mathcal{B}_\infty^n$ *boundaries,*

$$|\zeta_{n,R,S}\rangle := \sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n}\rho_R(\mathbf{y})\cdot e^{-\pi i\frac{\|\mathbf{y}\|^2}{S^2}}\,|\mathbf{y}\rangle\,,\quad \left|\zeta^{\infty}_{n,R,S}\right\rangle := \sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\log n\mathcal{B}_\infty^n}\rho_R(\mathbf{y})\cdot e^{-\pi i\frac{\|\mathbf{y}\|^2}{S^2}}\,|\mathbf{y}\rangle$$

can both be prepared in $\mathrm{poly}(n)$ *time within trace distances* $2^{-\Omega(n)}$*.*

Proof. We describe how to prepare $|\zeta_{n,R,S}\rangle$. The procedure for preparing $\left|\zeta^{\infty}_{n,R,S}\right\rangle$ is similar.

To prepare $|\zeta_{n,R,S}\rangle$ we start from preparing the Gaussian state $|\sigma_{n,R}\rangle$ using Lemma 2.14, and then apply Lemma 2.13 to change the phase:

$$\sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n}\rho_R(\mathbf{y})\,|\mathbf{y}\rangle\mapsto\sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n}\rho_r(\mathbf{y})\cdot e^{-\pi i\frac{\|\mathbf{y}\|^2}{S^2}}\,|\mathbf{y}\rangle =: \left|\zeta'_{n,R,S}\right\rangle.$$

$\left|\zeta'_{n,R,S}\right\rangle$ and $|\zeta_{n,R,S}\rangle$ are $2^{-\Omega(n)}$-close in the ℓ_2 distance because the normalization factor of both $\left|\zeta'_{n,R,S}\right\rangle$

and $|\zeta_{n,R,S}\rangle$ is $\sqrt{\sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n}\rho_R^2(\mathbf{y})}$, and

$$\begin{aligned}
\| \left|\zeta'_{n,R,S}\right\rangle - |\zeta_{n,R,S}\rangle \|_2^2 &= \sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n} \left|\rho_R(\mathbf{y})\cdot\left(e^{-\pi i\frac{\|\mathbf{y}\|^2}{\tilde{S}^2}} - e^{-\pi i\frac{\|\mathbf{y}\|^2}{S^2}}\right)\right|^2 \\
&= \sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n} \left|\rho_R(\mathbf{y})\cdot e^{-\pi i\frac{\|\mathbf{y}\|^2}{\tilde{S}^2}}\left(1 - e^{-\pi i\cdot(1/S^2-1/\tilde{S}^2)\cdot\|\mathbf{y}\|^2}\right)\right|^2 \\
\in_{(a)} &\sum_{\mathbf{y}\in\mathbb{Z}^n\cap R\sqrt{n}\mathcal{B}_2^n} \rho_R^2(\mathbf{y})\cdot 2^{-\Omega(n)},
\end{aligned}$$

where (a) holds since $\|\mathbf{y}\|^2 \le R^2\cdot n$, so $(1/S^2 - 1/\tilde{S}^2)\cdot\|\mathbf{y}\|^2 \in 2^{-\Omega(n)}$. □

We will also use a trick called "domain extension". Let us first define periodic functions.

Definition 2.16 (Periodic function)**.** *Let $n, P \in \mathbb{N}^+$. A function $f : \mathbb{Z}^n \to \mathbb{C}$ is P-periodic if for all $\mathbf{x},\mathbf{y}\in\mathbb{Z}^n$ such that $\mathbf{x}\equiv\mathbf{y} \pmod P$, $f(\mathbf{x}) = f(\mathbf{y})$.*

Lemma 2.17 (Domain extension)**.** *Let $n, P, C \in \mathbb{N}^+$. Let $f : \mathbb{Z}^n \to \mathbb{C}$ be a P-periodic function. Then, there is an efficient reversible operation that given a quantum state $|\phi\rangle := \sum_{\mathbf{x}\in\mathbb{Z}_P^n} f(\mathbf{x})\,|\mathbf{x}\rangle$, converts it to $|\phi'\rangle := \sum_{\mathbf{z}\in\mathbb{Z}_{CP}^n} f(\mathbf{z})\,|\mathbf{z}\rangle$ in time $\mathrm{poly}(\log(C), n)$. Similarly, we can also convert $|\phi\rangle$ to $|\phi''\rangle := \sum_{z_1\in\mathbb{Z}_{CP},\mathbf{z}_{[2\ldots n]}\in\mathbb{Z}_P^{n-1}} f(\mathbf{z})\,|\mathbf{z}\rangle$, where the extension only applies on the first coordinate.*

Proof. We prepare a uniform superposition over $\mathbb{Z}_C^n$ by $\mathsf{QFT}_{\mathbb{Z}_C^n}|0^n\rangle = \sum_{\mathbf{h}\in\mathbb{Z}_C^n}|\mathbf{h}\rangle$, and interpret it as the higher order bits of $|\phi\rangle$:

$$\sum_{\mathbf{h}\in\mathbb{Z}_C^n}|\mathbf{h}\rangle\otimes|\phi\rangle \mapsto \sum_{\mathbf{h}\in\mathbb{Z}_C^n}\sum_{\mathbf{x}\in\mathbb{Z}_P^n} f(\mathbf{x})\,|\mathbf{h}\cdot P+\mathbf{x}\rangle =_{(a)} \sum_{\mathbf{z}\in\mathbb{Z}_{CP}^n} f(\mathbf{z})\,|\mathbf{z}\rangle = \left|\phi'\right\rangle,$$

where (a) holds since f is P-periodic. To get back to $|\phi\rangle$ from $|\phi'\rangle$, we apply $\mathsf{QFT}_{\mathbb{Z}_C^n}^{-1}$ on the higher order bits of $|\phi'\rangle$ and get $|0^n\rangle\,|\phi\rangle$.

Analogously, to get $|\phi''\rangle$, we prepare $\sum_{h_1\in\mathbb{Z}_C}|h_1\rangle$ and interpret it as the higher order bits of the first coordinate of $|\phi\rangle$:

$$\sum_{h_1\in\mathbb{Z}_C}|h_1\rangle\otimes|\phi\rangle \mapsto \sum_{h_1\in\mathbb{Z}_C}|h_1\rangle\sum_{\mathbf{x}\in\mathbb{Z}_P^n} f(\mathbf{x})\,|h_1\cdot P+x_1\rangle\left|\mathbf{x}_{[2\ldots n]}\right\rangle = \sum_{z_1\in\mathbb{Z}_{CP},\mathbf{z}_{[2\ldots n]}\in\mathbb{Z}_P^{n-1}} f(\mathbf{z})\,|\mathbf{z}\rangle = \left|\phi''\right\rangle.$$

□

3 Main Theorem: Quantum Algorithm for Solving LWE

This section is devoted to proving the main theorem:

Theorem 3.1. *Let $\ell, m, q \in \mathbb{N}$, $\beta \ge 2$ such that $m \ge \Omega(\ell\log_2(q))$, $q \in \tilde{\Omega}(\beta^4 m^2)$. There is a quantum algorithm that solves $\mathsf{LWE}_{\ell,m,q,U(\mathbb{Z}_q),D_{\mathbb{Z},\beta}}$ in time $\mathrm{poly}(m, \log q, \beta)$.*

The rest of the section is organized as follows. In §3.1 we show LWE with k secret coordinates chosen by ourselves, denoted as $\mathsf{LWE}^{k \text{ chosen secret}}$, is as hard as standard LWE ($\mathsf{LWE}^{k \text{ chosen secret}}$ will be solved quantumly later). In §3.2 we convert $\mathsf{LWE}^{k \text{ chosen secret}}$ into the problem of finding the unique shortest non-zero vector of a special q-ary lattice. In §3.3 we list the parameters that are used in the main quantum algorithm. In §3.4 we provide an overview of the main quantum algorithm. In §3.5 we provide the nine steps in the main quantum algorithm in details, but deferring all proofs that are longer than three pages to §3.6. In §3.6 we provide all the detailed proofs missed in §3.5.

3.1 LWE with a few known secret coordinates is as hard as standard LWE

We show three variants of LWE that are as hard as standard LWE. The last variant is $\mathsf{LWE}^{k \text{ chosen secret}}$ (formally defined in Def. 3.4), which our quantum algorithm will eventually solve. All three reductions in this subsection follow small modifications of existing classical polynomial time reductions from the standard LWE to their variants.

1: LWE with k error free coordinates. First, we convert the standard LWE into a variant of it where the first k coordinates of the error term is 0, denoted as $\mathsf{LWE}^{k \text{ error free}}$. Analogously, for the decisional version, $\mathsf{DLWE}^{k \text{ error free}}$, we assume the first k coordinates of the error term is 0 in the LWE case, and the RANDOM case is still all random. (Although we only need the search version of $\mathsf{LWE}^{k \text{ error free}}$ in this paper, we present the reduction for the decisional version because it implies the search version and might be useful elsewhere). Brakerski et al. [BLP+13] prove that $\mathsf{LWE}^{1 \text{ error free}}$ is as hard as standard LWE. We generalize their proof to a larger k. Apparently, for $\mathsf{LWE}^{k \text{ error free}}$ to be hard, k cannot be larger than the dimension of the secret. In fact, the reduction actually transforms an n-dimensional LWE instance to an $n+k$ dimensional $\mathsf{LWE}^{k \text{ error free}}$ instance, so having k error free coordinates do not make the problem simple.

Lemma 3.2. *For any $k, n, m, q \in \mathbb{N}$ such that $k \in \text{poly}(n), q \leq 2^{\text{poly}(n)}$, there is a reduction from $\mathsf{DLWE}_{n,m,q,U(\mathbb{Z}_q),\chi}$ to $\mathsf{DLWE}^{k \text{ error free}}_{n+k,m+k,q,U(\mathbb{Z}_q),\chi}$ that runs in classical $\text{poly}(k, n, m, \log q)$ time and reduces the advantage by at most $2^{-\Omega(n)}$.*

Proof. Suppose $q = q_1^{c_1}...q_h^{c_h}$, where $q_1, ..., q_h$ are h distinct primes, $c_1, ..., c_h \in \mathbb{N}$. Given an instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}, \mathbf{t} \in \mathbb{Z}_q^m$ from $\mathsf{DLWE}_{n,m,q,U(\mathbb{Z}_q),\chi}$, we convert it to an instance of $\mathsf{DLWE}^{k \text{ error free}}_{n+k,m+k,q,U(\mathbb{Z}_q),\chi}$.

We first sample k vectors $\mathbf{u}_1$, ..., $\mathbf{u}_k \in \mathbb{Z}_q^{n+k}$ uniformly random. If $\mathbf{u}_1$, ..., $\mathbf{u}_k$ are linearly independent in $\mathbb{Z}_{q_i}$ for all $i \in [h]$, then we continue, otherwise we abort. The following claim says we abort with probability less than $k \log_2 q \cdot 2^{-n} \in 2^{-\Omega(n)}$.

Claim 3.3. *With probability more than $1 - k \log_2 q \cdot 2^{-n}$ over the randomness of sampling uniformly random $\mathbf{u}_1$, ..., $\mathbf{u}_k \in \mathbb{Z}_q^{n+k}$, $\mathbf{u}_1$, ..., $\mathbf{u}_k$ are linearly independent in $\mathbb{Z}_{q_i}$ for all $i \in [h]$.*

Proof. For every $i \in [h]$, $\mathbf{u}_1$, ..., $\mathbf{u}_k$ are linearly independent in $\mathbb{Z}_{q_i}$ with probability

$$(1 - q_i^{-(n+k)})(1 - q_i^{-(n+k-1)})...(1 - q_i^{-(n+1)}) \geq (1 - 2^{-n})^k.$$

Note that $h \leq \log_2 q$. So the probability that $\mathbf{u}_1$, ..., $\mathbf{u}_k$ are linearly independent in $\mathbb{Z}_{q_i}$ for all $i \in [h]$ is greater than $(1 - 2^{-n})^{k \log_2 q} \geq 1 - k \log_2 q \cdot 2^{-n}$. □

We then sample a matrix $\mathbf{U} \in \mathbb{Z}_q^{(n+k)\times(n+k)}$ that is invertible modulo q, and the first k columns of $\mathbf{U}$ are $\mathbf{u}_1$, ..., $\mathbf{u}_k$ ($\mathbf{U}$ only has to be invertible modulo q, not random). Such a matrix $\mathbf{U}$ exists and can be sampled efficiently as follows. Let $\mathbf{U}_{[1...k]} = (\mathbf{u}_1, ..., \mathbf{u}_k)$. For every $i \in [h]$, we know there are k rows from $\mathbf{U}_{[1...k]}$ that forms an invertible matrix over $\mathbb{Z}_{q_i^{c_i}}$, then we can set $\mathbf{U}_{[k+1...n+k]} \bmod q_i^{c_i}$ to be 0 in those k rows, and contain an identity matrix besides those k rows, therefore the whole matrix $\mathbf{U}$ is invertible modulo $q_i^{c_i}$ (for example, if the first k rows in $\mathbf{U}_{[1...k]}$ form an invertible matrix $\bmod q_i^{c_i}$, then we let $\mathbf{U}_{[k+1...n+k]} = \begin{pmatrix} \mathbf{0} \\ \mathbf{I}_n \end{pmatrix} \bmod q_i^{c_i}$). Using the Chinese remainder theorem, we get $\mathbf{U}$ as an invertible matrix over $\mathbb{Z}_q$.

Then, for the j^{th} sample of $\mathsf{DLWE}^{k \text{ error free}}_{n+k,m,q,U(\mathbb{Z}_q^{n+k}),\chi}$, for $j \in [k]$, we output $\mathbf{u}_j$, y_j, where y_j is sampled randomly from $\mathbb{Z}_q$. Denote $\mathbf{y} \in \mathbb{Z}_q^k$ as the concatenation of y_1, ..., y_k. For $j = k+1, ..., m+k$, we sample a uniformly random vector $\mathbf{d}_j \in \mathbb{Z}_q^k$, and output $\mathbf{U}\begin{pmatrix} \mathbf{d}_j \\ \mathbf{a}_{j-k} \end{pmatrix}$, $t_{j-k} + \langle \mathbf{d}_j, \mathbf{y} \rangle$.

It is easy to verify that the reduction maps a RANDOM instance of $\mathsf{DLWE}_{n,m,q,U(\mathbb{Z}_q^n),\chi}$ to a RANDOM instance of $\mathsf{DLWE}^{k \text{ error free}}_{n+k,m+k,q,U(\mathbb{Z}_q^{n+k}),\chi}$. To verify the LWE case, suppose $\mathbf{t} = \mathbf{A}^T\mathbf{s}+\mathbf{e}$, then the secret term of the new instance is $\mathbf{s}' := \mathbf{U}^{-T}\begin{pmatrix} \mathbf{y} \\ \mathbf{s} \end{pmatrix}$. So for $j \in [k]$, the j^{th} sample is $\mathbf{u}_j, \langle \mathbf{u}_j, \mathbf{s}' \rangle = y_j$, free of error; for $j = k+1, ..., m+k$, the j^{th} sample is $\mathbf{a}'_j := \mathbf{U}\begin{pmatrix} \mathbf{d}_j \\ \mathbf{a}_{j-k} \end{pmatrix}$, $t_{j-k} + \langle \mathbf{d}_j, \mathbf{y} \rangle = e_{j-k} + \langle \mathbf{a}_{j-k}, \mathbf{s} \rangle + \langle \mathbf{d}_j, \mathbf{y} \rangle = e_{j-k} + \left\langle \mathbf{a}'_j, \mathbf{s}' \right\rangle$, following the right distribution. □

2: LWE with k chosen error terms. Next, we convert $\mathsf{LWE}^{k \text{ error free}}$ into a variant of it where the first k coordinates of the error terms are chosen by ourselves, instead of being 0. We denote this variant as $\mathsf{LWE}^{k \text{ chosen error}}$. This conversion is simple: staring from samples from $\mathsf{LWE}^{k \text{ error free}}$, denoted by $\mathbf{A} \in \mathbb{Z}_q^{n\times m}, \mathbf{y} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, where $\mathbf{e}_{[1...k]} = 0^k$. Let $\mathbf{z} \in \mathbb{Z}_q^k$ be the k error terms chosen by ourselves. We output $\mathbf{A}, \mathbf{y} + \mathbf{z}|0^{m-k} = \mathbf{A}^T\mathbf{s} + \mathbf{z}|\mathbf{e}_{[k+1...m]}$.

3: LWE where the secret follows the error distribution. Third, we apply the reduction of Applebaum et al. [ACPS09] which transforms LWE samples into new LWE samples where the secret follows the error distribution. As a result of this transformation, we convert $\mathsf{LWE}^{k \text{ chosen error}}_{n,m+n,q,U(\mathbb{Z}_q),\chi}$ into new LWE samples where the first k coordinates of the secret is chosen, and the rest of the secret and the error vectors follows the same error distribution of $\mathsf{LWE}^{k \text{ chosen error}}$. We call this variant $\mathsf{LWE}^{k \text{ chosen secret}}$.

Definition 3.4 (LWE with k chosen secrets)**.** *Let $k < n < m$, q be positive integers. Let $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector where the first k entries are chosen to be fixed as $(s_1, ..., s_k)$, and the other entries $(s_{k+1}, ..., s_n)$ are sampled from some distribution DistS and unknown. The problem $\mathsf{LWE}^{k \text{ chosen secret}}_{n,m,q,DistS,DistE}$ asks to find the secret $\mathbf{s}$ given access to an oracle that outputs $\mathbf{a}_i$, $\langle \mathbf{s}, \mathbf{a}_i \rangle + e_i \pmod q$ on its i^{th} query, for $i = 1, ..., m$. Here each $\mathbf{a}_i$ is a uniformly random vector in $\mathbb{Z}_q^n$, and each error term e_i is sampled from DistE over $\mathbb{Z}_q$.*

Lemma 3.5. *There is a classical reduction from $\mathsf{LWE}^{k \text{ chosen error}}_{n,m+n,q,U(\mathbb{Z}_q),\chi}$ to $\mathsf{LWE}^{k \text{ chosen secret}}_{n,m,q,\chi,\chi}$ that runs in time* $\mathrm{poly}(n, m, \log q)$.

Proof. Given $m+n$ samples from $\mathsf{LWE}^{k \text{ chosen error}}_{n,m+n,q,U(\mathbb{Z}_q),\chi}$, denoted as $\mathbf{A}, \mathbf{y}^T := \mathbf{s}^T\mathbf{A} + \mathbf{e}^T \bmod q$. Write $\mathbf{A} = [\mathbf{A}_1 \mid \mathbf{A}_2]$ where $\mathbf{A}_1 \in \mathbb{Z}_q^{n\times n}$, $\mathbf{A}_2 \in \mathbb{Z}_q^{n\times m}$. Without a loss of generality, assume $\mathbf{A}_1$ is invertible modulo q (we know the first k columns of $\mathbf{A}_1$ are part of an invertible matrix back from Lemma 3.2; if $\mathbf{A}_1$ is not invertible, we replace some columns from the last $n-k$ columns of $\mathbf{A}_1$ by some columns of $\mathbf{A}_2$ until we make $\mathbf{A}_1$ invertible; this does not affect our result). Write $\mathbf{y}^T = [\mathbf{y}_1^T \mid \mathbf{y}_2^T]$ where $\mathbf{y}_1 \in \mathbb{Z}_q^n$. Let $\bar{\mathbf{A}} := -\mathbf{A}_1^{-1}\cdot\mathbf{A}_2$. Let $\bar{\mathbf{y}}^T := \mathbf{y}_1^T\cdot\bar{\mathbf{A}}+\mathbf{y}_2^T$. Then $\bar{\mathbf{y}}^T = (\mathbf{s}^T\mathbf{A}_1+\mathbf{e}_1^T)\cdot(-\mathbf{A}_1^{-1}\cdot\mathbf{A}_2)+(\mathbf{s}^T\mathbf{A}_2+\mathbf{e}_2^T) = \mathbf{e}_1^T\cdot\bar{\mathbf{A}}+\mathbf{e}_2^T$, meaning that $\bar{\mathbf{A}}, \bar{\mathbf{y}}^T$ is an instance of $\mathsf{LWE}^{k \text{ chosen secret}}_{n,m,q,\chi,\chi}$, i.e., the secret for $\mathsf{LWE}^{k \text{ chosen secret}}_{n,m,q,\chi,\chi}$ is $\mathbf{e}_1 \in \mathbb{Z}_q^n$, which is sampled from the first n error coordinates of $\mathsf{LWE}^{k \text{ chosen error}}_{n,m+n,q,U(\mathbb{Z}_q),\chi}$. In particular, the first k secret terms are chosen by ourselves. □

3.2 Convert LWE into a special q-ary lattice with a unique shortest vector

Let $\kappa, \ell, m, q \in \mathbb{N}$, $m \in \Omega(\ell \log q)$, $n := 1+\ell+m$, $\kappa \le O(\log n)$. Let $p_1, p_2, p_3, ..., p_\kappa$ be odd and pairwise coprime, such that $p_1 \in O(1)$, $p_2, ..., p_\kappa \le \frac{\log n}{p_1}$. Note that $p_1, p_2, ..., p_\kappa$ don't have to be primes. Other conditions of $p_1, ..., p_\kappa$ will be mentioned later in §3.3 (mostly in Cond. **C.3**).

With the three reductions in §3.1, we know that to solve standard $\mathsf{LWE}_{\ell-(\kappa-1),m+\ell-(\kappa-1),q,U(\mathbb{Z}_q),D_{\mathbb{Z},\beta}}$, it suffices to solve $\mathsf{LWE}^{\kappa-1 \text{ chosen secret}}_{\ell,m,q,D_{\mathbb{Z},\beta},D_{\mathbb{Z},\beta}}$. More concretely, let the $\mathsf{LWE}^{\kappa-1 \text{ chosen secret}}_{\ell,m,q,D_{\mathbb{Z},\beta},D_{\mathbb{Z},\beta}}$ instance be $\mathbf{U} \leftarrow U(\mathbb{Z}_q^{\ell\times m})$, $\mathbf{t} = \mathbf{U}^T\mathbf{s}+\mathbf{e} \bmod q$, where the first $\kappa-1$ entries $\mathbf{s}$ are chosen to be $(p_2, ..., p_\kappa)$, and the other $\ell-(\kappa-1)$ entries of $\mathbf{s}$, $\mathbf{s}_{[\kappa...\ell]}$, and all entries of the error term $\mathbf{e}$ are sampled independently from $D_{\mathbb{Z},\beta}$. Our goal is to compute the unknown $\mathbf{s}_{[\kappa...\ell]}$ and $\mathbf{e}$.

Looking ahead, the property that we choose $\kappa-1$ coordinates of the secret to be some known, special values will only be used at the very last step of our quantum algorithm, so readers on the first pass of our algorithm can just assume we are solving LWE where the secret and the error terms are all small entries (i.e., all less than $O(\beta \log n)$) and not worry about the condition that $\kappa-1$ entries are special values, until reaching the last step of our quantum algorithm.

We now define a q-ary lattice such that finding the unique shortest vector for this special q-ary lattice implies solving $\mathsf{LWE}^{\kappa-1 \text{ chosen secret}}_{\ell,m,q,D_{\mathbb{Z},\beta},D_{\mathbb{Z},\beta}}$. Let

$$\begin{aligned} \mathbf{A} &:= [2p_1\mathbf{t} \mid \mathbf{U}^T \mid \mathbf{I}_m] \in \mathbb{Z}_q^{m\times n}, \\ \mathbf{b} &:= [-1, 2p_1\mathbf{s}^T, 2p_1\mathbf{e}^T]^T = [-1, 2p_1p_2, ..., 2p_1p_\kappa, 2p_1\mathbf{s}_{[\kappa...\ell]}^T, 2p_1\mathbf{e}^T]^T. \end{aligned} \tag{12}$$

Note that $\mathbf{Ab} \equiv \mathbf{0} \bmod q$.

Let us first provide some basic estimations of the length of $\mathbf{b}$.

Lemma 3.6. *For $\beta \ge 2$, $p_1 \in O(1)$, $p_2, ..., p_\kappa \le \frac{\log n}{p_1}$, $\kappa \in O(\log n)$. With probability $1-\mathrm{negl}(n)$ over the randomness in sampling $\mathbf{s}_{[\kappa...\ell]} \leftarrow D_{\mathbb{Z},\beta}^{\ell-\kappa+1}, \mathbf{e} \leftarrow D_{\mathbb{Z},\beta}^m$, the vector $\mathbf{b} = [-1, 2p_1\mathbf{s}^T, 2p_1\mathbf{e}^T]^T$ satisfies (1) $\|\mathbf{b}\| \le 3p_1\beta\sqrt{n}$, (2) $\|\mathbf{b}\|_\infty \le \beta \log n$, and (3) $\|\mathbf{b}\|^2 \in 1+4p_1^2(p_2^2+...+p_\kappa^2)+[0.04, 0.27]\cdot 4p_1^2\beta^2(n-\kappa)$.*

Proof. From Lemma 2.5, we know $\|\mathbf{b}\| \le 2p_1\beta\sqrt{n-\kappa}+O(\log^2 n) \le 3p_1\beta\sqrt{n}$ with probability $1-2^{-\Omega(n)}$. From Lemma 2.6, we know $\|\mathbf{b}\|_\infty \le \beta \log n$ with probability $1-\mathrm{negl}(n)$. So Items (1), (2) are satisfied.

To prove Item (3), given that $\beta \ge 2$, and $\eta_{0.086434811}(\mathbb{Z}) \ge 1$, we derive from Lemma 2.9 that for $i = \kappa+1, ..., n$, $\mathbb{E}[\frac{b_i^2}{(2p_1)^2}] \in \frac{\beta^2}{2\pi} \pm 0.09\beta^2 \in [0.05, 0.26]\cdot\beta^2$. Also, by Lemma 2.6, $0 \le \frac{b_i^2}{(2p_1)^2} \le \beta^2\log^2(n-\kappa)$.

Then, using Hoeffding inequality (Lemma 2.2), we let $S_{n-\kappa} := \sum_{i=\kappa+1}^{n} \frac{b_i^2}{(2p_1)^2}$, then

$$\Pr\left[|S_{n-\kappa} - \mathbb{E}[S_{n-\kappa}]| \geq \beta^2 \log^3(n-\kappa)\sqrt{n-\kappa}\right] \leq 2e^{-\frac{2(n-\kappa)\beta^4 \log^6(n-\kappa)}{(\beta^2 \log^2(n-\kappa))^2 \cdot (n-\kappa)}} \in \text{negl}(n).$$

Therefore $\|\mathbf{b}\|^2 \in 1 + 4p_1^2(p_2^2 + ... + p_\kappa^2) + [0.04, 0.27] \cdot 4p_1^2\beta^2(n-\kappa)$ with all but negl(n) probability. □

In Lemma 3.7, we prove that $\mathbf{b}$ is the unique shortest vector in $L_q^\perp(\mathbf{A})$, whereas other vectors in $L_q^\perp(\mathbf{A})$ are long. The proof is not hard but a bit tedious so we defer it to §3.6.1. Looking ahead, our quantum algorithm is essentially trying to compute $\mathbf{b}$, the unique shortest non-zero vector in $L_q^\perp(\mathbf{A})$.

Lemma 3.7. *For $q \geq \tilde{\Omega}(\beta^4 m^2)$. With probability $1 - \text{negl}(n)$ over the randomness in sampling $\mathbf{U}$, $\mathbf{t}$, $\lambda_1\left(L_q^\perp(\mathbf{A})\right) = \|\mathbf{b}\| \leq 3p_1\beta\sqrt{n}$, $\lambda_2^\infty\left(L_q^\perp(\mathbf{A})\right) \geq q/(\log n)^2$.*

Note that if $q \in 2p_1\mathbb{Z}$, then $\frac{q}{2p_1}|0^{n-1}$ is a relatively short vector in $L_q^\perp(\mathbf{A})$ (not shorter than $\mathbf{b}$ though). But since we set $p_1 \in O(1)$, so $\frac{q}{2p_1} > \frac{q}{\log^2 n}$, which doesn't violate Lemma 3.7. So we don't need to avoid q, p_1 such that $q \in 2p_1\mathbb{Z}$.

3.3 Parameter selection

Recall that in §3.2 we have defined parameters $\ell, m, q, n = 1 + m + \ell, p_1, ..., p_\kappa$, and the q-ary lattice $\mathbf{A} = [2p_1\mathbf{t} \mid \mathbf{U}^T \mid \mathbf{I}_m] \in \mathbb{Z}_q^{m \times n}$, where $\mathbf{t} = \mathbf{U}^T\mathbf{s} + \mathbf{e} \mod q$ where $\mathbf{s}_{[1...\kappa-1]} = (p_2, ..., p_\kappa)$, $\mathbf{s}_{[\kappa...\ell]} \leftarrow D_{\mathbb{Z},\beta}^{\ell-\kappa+1}, \mathbf{e} \leftarrow D_{\mathbb{Z},\beta}^m$. Recall from Eqn. (12) that $\mathbf{b} = [-1, 2p_1\mathbf{s}^T, 2p_1\mathbf{e}^T]^T$.

In this subsection we introduce more parameters that will be used in our quantum algorithm. Let $D \in \mathbb{N}^+$ be a scaling parameter. Let $L := D \cdot L_q^\perp(\mathbf{A})$. Let $\mathbf{x} := D \cdot \mathbf{b}$.

We set additional parameters $P, M, r, s, t, u \in \text{poly}(n)$ such that $P, M, t^2, u^2 \in \mathbb{N}^+$, $s, r \in \mathbb{R}^+$. P, M are the large and small moduli. The main parameters for complex Gaussian are r, s, t, u. Our algorithm will first make a guess of $\|\mathbf{b}\|^2 \in \mathbb{N}^+$ and let $u^2 = \|\mathbf{x}\|^2 = D^2\|\mathbf{b}\|^2$. There are only $O(\beta^2 n) \in \text{poly}(n)$ possibilities for $\|\mathbf{b}\|^2$, so from now we assume our guess of $\|\mathbf{b}\|^2$ is correct.

The parameters are set under the following constraints (readers can assume we always use $P > r > M > s > t > u = \|\mathbf{x}\| = D\|\mathbf{b}\|$). Looking ahead, there are nine steps in our quantum algorithm, and each condition below is typically only used in one or few steps. We will mark which condition is used in which steps, so readers don't need to load all the conditions in mind at the same time, and just assume all conditions are satisfiable on the first pass.

- **C.1** $t^2 = cu^2$ for some $c \in 4\mathbb{Z}$. This ensures that $\frac{t^2}{2D^2} = \frac{cD^2\|\mathbf{b}\|^2}{2D^2} \in 2\mathbb{Z}$ (only used in Lemma 3.27 in Step 6). For simplicity we set $\frac{t}{u} = \sqrt{c} \in (64\log^3 n, 65\log^3 n)$, then **C.6**, **C.7** are easy to satisfy.
- **C.2** The large and small moduli P, M are chosen as $M = 2(t^2+u^2) = 2(c+1)\|\mathbf{x}\|^2 = 2(c+1)D^2\|\mathbf{b}\|^2$, $P = M \cdot (t^2+u^2) = \frac{M^2}{2}$. This condition is used in many steps.
- **C.3** (Only used in Steps 8 and 9.) D, p_1, p_2, ..., p_κ are odd and pairwise coprime (they don't have to be primes), $\frac{M}{2D^2} = (c+1)\|\mathbf{b}\|^2 = p_1p_2...p_\kappa$, and $p_2p_3...p_\kappa \equiv -1 \pmod{p_1}$. Since $M \in \text{poly}(n)$, therefore $\kappa \in O(\log n)$ is enough (i.e., M has at most $O(\log n)$ different factors).

C.4 $2r\log n \le P$, $2r\log n < Dq/(\log n)^2$ (only used in Step 1). Note that $2r\log n < Dq/(\log n)^2$ is the only constraint on q. In particular, q does not have to be equal to or share prime factors with P or any other values.

C.5 The key condition for creating the Karst wave: $\frac{s^2r^4}{u^2(s^4+r^4)}\frac{t^2}{(t^2+u^2)^2} = 2$ (mainly used in Step 6). Since we always set $r > s\log n$, $t \ge 64u\log^3 n$, we have $s^2 = 2\frac{u^2(s^4+r^4)}{r^4}\frac{(t^2+u^2)^2}{t^2} \in 2u^2t^2\cdot\left(1, 1+\frac{1}{\log n}\right)$.

C.6 Define $V := \frac{Pu\sqrt{r^4+s^4}}{rs^2t}$ (only used in Step 3), $\sigma := \frac{P}{V} = \frac{rs^2t}{u\sqrt{r^4+s^4}} \in \frac{ts^2}{ur}\cdot\left(1\pm\frac{1}{O(\log n)}\right) \in_{\mathbf{C.5}} \frac{2ut^3}{r}\cdot\left(1\pm\frac{1}{O(\log n)}\right)$ (σ is used in Steps 6 and 7). We need $\sigma \in \left(2\log n, \frac{D}{4\log n}\right)$.

C.7 $\frac{2ut^2}{r} < \frac{1}{4\beta\sqrt{n}\log^2 n}$, needed in Steps 5 and 7. Since $u = D\|\mathbf{b}\| \ge_{Lemma\ 3.6(3)} \frac{\beta\sqrt{n}}{4}$ with all but negl(n) probability, it suffices to set $\frac{u^2t^2}{r} < \frac{1}{32\log^2 n}$. Combining with **C.6**, where we need $\frac{2ut^3}{r}\cdot\left(1\pm\frac{1}{O(\log n)}\right) \in \left(\log n, \frac{D}{4\log n}\right)$. Since we set $\frac{t}{u} = \sqrt{c} \in (64\log^3 n, 65\log^3 n)$ in **C.1**, we can set $r = \frac{ut^3}{4\log n}$, $\sigma \in O(\log n)$, and $D \in O(\log^2 n)$ so that both **C.6**, **C.7** are satisfied.

We can determine all parameters in the following order: first choose $c+1$, p_1, p_2, ..., p_κ to make sure **C.3** is satisfiable, namely, $(c+1)\|\mathbf{b}\|^2 = p_1p_2...p_\kappa$. Note that $\mathbf{b}_{[1...\kappa]} = (-1, 2p_1p_2, ..., 2p_1p_\kappa)$, and $\mathbf{b}_{[\kappa+1...n]} \in 2p_1$, so $\|\mathbf{b}\|^2 = 1+4p_1^2(p_2^2+p_3^2+...+p_\kappa^2+a)$ for some $a \in \mathbb{Z}$ such that $a \approx \frac{\beta^2}{2\pi}(n-\kappa)$ (there are only $O(\beta^2(n-\kappa)) \in$ poly(n) possibilities of a, so we can guess a to be the most likely value of $\frac{\|\mathbf{b}_{[\kappa+1...n]}\|^2}{4p_1^2}$, i.e., $\left\lfloor\frac{\beta^2}{2\pi}(n-\kappa)\right\rceil$, then with non-negligible probability over the randomness of $\mathbf{b}_{[\kappa+1...n]}$, our guess of $\|\mathbf{b}\|^2$ is correct). Also note that $\|\mathbf{b}\|^2 \notin p_1\mathbb{Z}$. So the easiest solution is to set p_1 to be a factor of $c+1$, and guess $\|\mathbf{b}\|^2$ has some smooth factors $p_2...p_\kappa$. For example, if we guess $\|\mathbf{b}\|^2 = 7\times11\times17\times19\times31 = 771001$, and set $p_1 = 5$, then $\|\mathbf{b}\|^2 = 1+100(7^2+11^2+17^2+19^2+31^2+a) = 1+100(1781+a)$ is satisfiable for some $a \in \mathbb{Z}$.

We then pick an odd number $D \in O(\log^2 n)$, and let $u^2 = D^2\|\mathbf{b}\|^2$. Then u^2 and $(c+1)$ determines t^2, which then determines M, P, r, and we finally compute s according to **C.5** (we don't need s or s^2 to be rational, we only need to compute s within sufficient precision in order to use Lemma 2.15 to prepare complex Gaussian states).

Since we assume $\beta \ge 2$, then by Lemma 3.6, the minimum of $\|\mathbf{b}\|^2$ is $0.04\cdot4p_1^2\beta^2(n-\kappa)+1$ with all but negl(n) probability. We summarize this condition and its implications as follows

C.8 $\|\mathbf{b}\| \ge O(\sqrt{n})$, so $\frac{M}{2} \ge_{\mathbf{C.1}} u^2\log^6 n >_{\|\mathbf{b}\|\ge O(\sqrt{n}),\mathbf{C.7}} 4\|\mathbf{b}\|\sigma\sqrt{n}\log n$, $\frac{M}{r} \in_{\mathbf{C.7}} O\left(\frac{\log^4 n}{t^2}\right) < O\left(\frac{1}{n}\right)$.

To get the best approximation factors for general lattice problems, we aim at solving $\mathsf{LWE}^{\kappa-1\text{ chosen secret}}_{\ell,m,q,D^\ell_{\mathbb{Z},\beta},D_{\mathbb{Z},\beta}}$ where $m \in O(\ell\log q)$, $\beta = 2\sqrt{\ell}$, $q \in \tilde{O}(\ell^4)$, implying $n \in O(\ell\log\ell)$. Then we set

- $u^2 = \|\mathbf{x}\|^2 \in D^2\cdot O(\beta^2 n) \in \tilde{O}(n^2)$, $t^2 \in O(\log^6 n)\cdot u^2 \in \tilde{O}(n^2)$, $M \in O(t^2) \in \tilde{O}(n^2)$,
- $r \in O\left(\frac{t^4}{\log^4 n}\right) = O\left(u^4\log^8 n\right) \in \tilde{O}(n^4)$, $q \in O\left(u^4\log^9 n\right) \in \tilde{O}(n^4)$, $P \in O(t^4) \in \tilde{O}(n^4)$.

Then all parameter constraints are satisfiable. Readers on the first pass of the algorithm can keep this set of parameters in mind. To get quantum algorithms for general lattice problems using Lemma 1.5, we plug in $\alpha = \tilde{O}(n^{-3.5})$, yielding quantum algorithms that solve SIVP_γ and GapSVP_γ for all n-dimensional lattices for $\gamma \in \tilde{O}(n^{4.5})$.

We would like to mention that some constraints of parameters can be relaxed. For example, we believe if we use more sophisticated Gaussian tail bound proof techniques to prove Lemma 3.24, then **C.7** can be relaxed to $\frac{2ut^2}{r} < \frac{1}{4\beta \log^2 n}$, saving another factor of $\sqrt{n}$. But improving this bound would take more technical effort while not helping improve the approximation factor achieved by our algorithm, so we leave the loose bound in Cond. **C.7** as it is. Also, most of the $\log n$ factors appeared in the parameters can be changed to $\omega(\sqrt{\log n})$ because they are the byproduct of Lemma 2.6. But we are not aiming at optimizing polylog(n) factors, so we simply use $\log n$ to keep the write-up clear.

3.4 Detailed overview of the main quantum algorithm

After setting up the parameters as in §3.3, we run a quantum subroutine consisting of nine steps for $O(n)$ times. Every time we run the quantum subroutine, we will obtain a classical linear equation with random coefficients over the shortest vector in $L_q^\perp(\mathbf{A})$ (related to the LWE secret and error vectors). Therefore after running it for $O(n)$ times we will get a full rank system of linear equations and compute the LWE secret and error terms by Gaussian elimination.

Let us first provide a high level description of the nine steps in the quantum subroutine, including the state and classical information obtained in each step. We use $|\varphi_i\rangle$ to denote the quantum state obtained at the end of Step i. The classical information obtained in Steps 1, 3, 5, 8 will be used in later steps, so we mention where they are used to help readers keep track on them.

1. Prepare a uniform superposition over $L \cap \mathbb{Z}_{Dq}^n$, and then apply a complex Gaussian window on it. We obtain a classical string $\mathbf{y}' \in \mathbb{Z}_{Dq}^n$ and a quantum state $|\varphi_1\rangle$:
$$|\varphi_1\rangle = \sum_{k\in\mathbb{Z}, k\mathbf{x}-\mathbf{y}\in(r\log n)\mathcal{B}_\infty^n} \exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)\|k\mathbf{x}-\mathbf{y}\|^2\right)|k\mathbf{x}-\mathbf{y}\rangle\,, \tag{13}$$
where $\mathbf{y} \in \mathbb{Z}^n$ is an unknown vector at this moment but its information is carried in $\mathbf{y}'$.
2. Compute $|\varphi_2\rangle = \mathsf{QFT}_{\mathbb{Z}_P^n}|\varphi_1\rangle$.
3. Apply a complex Gaussian window on $|\varphi_2\rangle$, get $|\varphi_3\rangle$, $\mathbf{z}' \in \mathbb{Z}_P^n$.
4. Compute $|\varphi_4\rangle = \mathsf{QFT}_{\mathbb{Z}_P^n}|\varphi_3\rangle$.
5. Split $|\varphi_4\rangle$ into higher and lower order bits, then measure the lower order bits in $\mathbb{Z}_{t^2+u^2}^n$ and get $\mathbf{h}^* \in \mathbb{Z}_{t^2+u^2}^n$. Denote the residual state (containing the higher order bits in $\mathbb{Z}_M^n$) as $|\varphi_5\rangle$.
6. Compute $|\varphi_6\rangle = \mathsf{QFT}_{\mathbb{Z}_M^n}|\varphi_5\rangle$. (The Karst wave feature is heavily used in the analysis of Step 6.)
7. Extract the centers of the Gaussian ball states in $|\varphi_6\rangle$ using $\mathbf{y}'$, $\mathbf{z}'$, and $\mathbf{h}^*$, get
$$|\varphi_7\rangle = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} e^{2\pi i\frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{x}+\mathbf{v}'+\frac{M}{2}\mathbf{k} \bmod M\right\rangle, \tag{14}$$

where $\mathbf{v}'$ is a vector in L fixed by the previous measurements but unknown at this point.

8. Apply a sequence of small operations to extract $v_1' \bmod D^2 p_1$, without collapsing the state, and get $|\varphi_8\rangle = |\varphi_7\rangle$.

9. From $|\varphi_8\rangle$, use the $p_2, ..., p_\kappa$ values planted in the secret vector in the instance of $\mathsf{LWE}^{k \text{ chosen secret}}$, $v_1' \bmod D^2 p_1$ obtained in Step 8, and apply a few operations on $|\varphi_8\rangle$ to get a random vector $\mathbf{u} \in \mathbb{Z}^n_{\frac{M}{2}}$ satisfying

$$u_1 + \left\langle \mathbf{b}^*_{[2...n]}, \mathbf{u}_{[2...n]} \right\rangle \equiv 0 \pmod{\frac{M}{2D^2}}, \tag{15}$$

where in $\mathbf{b}^*_{[2...n]} = \mathbf{b}^*_{[2...\kappa]} | \mathbf{b}^*_{[\kappa+1...n]}$, $\mathbf{b}^*_{[2...\kappa]}$ is known and fixed, $\mathbf{b}^*_{[\kappa+1...n]} = \mathbf{b}_{[\kappa+1...n]}$, which is exactly the secret term we want to learn.

We summarize the nine steps above in the following statement:

Lemma 3.8. *There is a* $\mathrm{poly}(n)$ *time quantum algorithm that takes as input* $L_q^\perp(\mathbf{A})$*, where* $\mathbf{A}$ *is defined in Eqn.* (12)*, outputs a random vector* $\mathbf{u} \in \mathbb{Z}^n_{\frac{M}{2}}$ *that satisfies Eqn.* (15)*.*

Since $\|\mathbf{b}_{[\kappa+1...n]}\|_\infty \leq 2p_1 \cdot \beta \log n < \frac{M}{2D^2}$, solving a system of the modular linear equations in Eqn. (15) recovers $\mathbf{b}_{[\kappa+1...n]}$ completely. Therefore after collecting $O(n)$ random vectors $\mathbf{u} \in \mathbb{Z}^n_{\frac{M}{2}}$ satisfying Eqn. (15), we recover $\mathbf{b}_{[\kappa+1...n]}$ using Gaussian elimination, thus solving the $\mathsf{LWE}^{\kappa-1 \text{ chosen secret}}_{\ell,m,q,D_{\mathbb{Z},\beta},D_{\mathbb{Z},\beta}}$ problem, which completes the proof of Theorem 3.1.

Let us now explain the intuition behind our algorithm, see Fig. 2 for a proof-of-concept example.

The purpose of Step 1 is to obtain a classical string $\mathbf{y}'$ and a complex Gaussian state $|\varphi_1\rangle$ in Eqn. (13). The support of $|\varphi_1\rangle$ is on a line in the same direction with the secret shortest vector $\mathbf{x}$. As mentioned in the introduction in §1.3, $|\varphi_1\rangle$ looks very similar to an instance of EDCP, but we are not expecting to finding out $\mathbf{x}$ using existing algorithms for EDCP at this point, so we continue.

The five steps from Steps 2 to 6 together make sure that the amplitude of $|\varphi_6\rangle$ in Step 6 is highly structural, consisting of small Gaussian balls. If we think of $|\varphi_1\rangle$ as in the time domain, then $|\varphi_2\rangle, |\varphi_3\rangle, |\varphi_6\rangle$ are in the frequency domain, and they should in general look chaotic if we don't set the parameters (Condition **C.5** in particular) carefully. However, we tune the parameters carefully so that the amplitude of $|\varphi_6\rangle$ is highly structural due to the feature of Karst wave.

The operations from Steps 3 to 5 serve for the purpose of *modulus splitting*, i.e., we split the large modulus P into $P = M \cdot (t^2 + u^2)$, and the state in Step 5 only contains the higher order bits from the state in Step 4. The purpose of modulus splitting can be seen from the Karst wave in Figure 1 (bottom right): the absolute value of the amplitude of a Karst wave is periodic over a smaller modulus than P. The intention of splitting the modulus is in fact originally motivated by a failed attempt of solving LWE directly from Step 2, which is explained later in §3.7.1. Readers who are curious about the motivation can take a look at §3.7.1, although it is unrelated to the actual algorithm that is working. Splitting the modulus in a useful way is non-trivial. As we will see in Step 3, where we apply a complex Gaussian window on $|\varphi_2\rangle$. The condition of $u^2 = \|\mathbf{x}\|^2$ is used starting from Step 3 (u^2 is a parameter in the complex Gaussian window in Step 3) – only when $u^2 = \|\mathbf{x}\|^2$, we can guarantee that the amplitude of $|\varphi_4\rangle$ splits clearly between its higher order bits in $\mathbb{Z}^n_M$ and lower order bits in $\mathbb{Z}^n_{t^2+u^2}$.

$|\varphi_6\rangle$ is an important state to understand so let us give more explanations about the patterns in the amplitude of $|\varphi_6\rangle$. From Figure 2-(f), we see that $|\varphi_6\rangle$ contains lines of Gaussian balls of small width σ, aligned in the direction of $\mathbf{x}$. We can then shift those Gaussian balls to make sure their centers are on $L \in D\mathbb{Z}^n$, and then use naive rounding to $D\mathbb{Z}^n$ to extract their centers and get $|\varphi_7\rangle$ (see Figure 2-(g)).

As we can see from the expression of $|\varphi_7\rangle$ in Eqn. (14), now we get an EDCP-like state with purely *imaginary* Gaussian amplitudes, which is much easier to work with. Imagine if we can learn one coordinate of $\mathbf{v}'$, then we can convert $|\varphi_7\rangle$ into a correct EDCP state with a known, "wide" amplitude, therefore by [CLZ22, Theorem 12], there is a polynomial time quantum algorithm for solving EDCP with known, wide amplitudes. This is an idea that inspires the design of the actual algorithm, but our actual algorithm is different, more down-to-earth, and does not rely on the knowledge of EDCP, so readers who are not familiar with EDCP don't need to worry about it.

Towards the goal of learning one coordinate of $\mathbf{v}'$, we first use the nice property of imaginary Gaussian (i.e., *center = phase*) to obtain partial information of v'_1 in Step 8 – we use the phase kickback trick to change the phase of $|\varphi_7\rangle$, see Figure 2-(h), and then take QFT to get a linear equation and learn about $v'_1 \bmod D^2 p_1$, see Figure 2-(i). Then in Step 9, we gain more information about $\mathbf{v}'$ using the $p_2, ..., p_\kappa$ values planted in the secret vector in the instance of $\mathsf{LWE}^{k \text{ chosen secret}}$. Finally, we are able to extract a modular linear equation about the LWE secret and error terms.

3.5 The main quantum subroutine

Now we start describing the detailed algorithm.

3.5.1 Step 1: Prepare a superposition over $L \cap \mathbb{Z}^n_{Dq}$ and apply a complex Gaussian window

Lemma 3.9. *There is a* $\mathrm{poly}(n)$ *time quantum algorithm that takes* $L = D \cdot L_q^\perp(\mathbf{A})$ *as input, outputs*

$$|\varphi_1\rangle = \sum_{k\in\mathbb{Z}, k\mathbf{x}-\mathbf{y}\in(r\log n)\mathcal{B}^n_\infty} \exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)\|k\mathbf{x}-\mathbf{y}\|^2\right)|k\mathbf{x}-\mathbf{y}\rangle\,,$$

and a string $\mathbf{y}' \in \mathbb{Z}^n_{Dq}$ *such that* $\mathbf{y}' = \mathbf{v}+\mathbf{y}$ *(the equation holds over* $\mathbb{Z}^n$*), where* $\mathbf{v} \in L$, $\mathbf{y} \in \mathbb{Z}^n \cap r\log n\mathcal{B}^n_\infty$.

Proof. Recall that $L = D \cdot L_q^\perp(\mathbf{A})$. We start from preparing a uniform superposition over $\mathbf{v} \in L \cap \mathbb{Z}^n_{Dq}$ and a complex Gaussian state

$$\sum_{\mathbf{v}\in L\cap\mathbb{Z}^n_{Dq}} |\mathbf{v}\rangle \otimes \sum_{\mathbf{y}\in\mathbb{Z}^n\cap(r\log n)\mathcal{B}^n_\infty} \rho_r(\mathbf{y})\cdot e^{\frac{-\pi i\|\mathbf{y}\|^2}{s^2}}|\mathbf{y}\rangle\,. \tag{16}$$

Here, the second register can be produced efficiently within $2^{-\Omega(n)}$ distance using Lemma 2.15. The first register, $\sum_{\mathbf{v}\in L\cap\mathbb{Z}^n_{Dq}}|\mathbf{v}\rangle$, can be produced by

$$\sum_{\mathbf{v}_1\in\mathbb{Z}_q^{\ell+1}} |\mathbf{v}_1\rangle|\mathbf{0}_m\rangle \mapsto \sum_{\mathbf{v}_1\in\mathbb{Z}_q^{\ell+1}} |\mathbf{v}_1\rangle\left|-\left(\mathbf{t}\mid\mathbf{U}^T\right)\cdot\mathbf{v}_1 \bmod q\right\rangle \mapsto_{\textit{multiply by } D} \sum_{\mathbf{v}\in L\cap\mathbb{Z}^n_{Dq}}|\mathbf{v}\rangle\,.$$

From the state in Eqn. (16), we add the first register to the second register:

$$\sum_{\mathbf{v}\in L\cap\mathbb{Z}^n_{Dq}} |\mathbf{v}\rangle \sum_{\mathbf{y}\in\mathbb{Z}^n\cap(r\log n)\mathcal{B}^n_\infty} \rho_r(\mathbf{y})\cdot e^{\frac{-\pi i\|\mathbf{y}\|^2}{s^2}} |\mathbf{y}+\mathbf{v} \bmod Dq\rangle \tag{17}$$

We then measure $|\mathbf{y}+\mathbf{v} \bmod Dq\rangle$ and denote the result as $\mathbf{y}'\in\mathbb{Z}^n_{Dq}$, then compute $|\mathbf{v}\rangle \mapsto |\mathbf{v}-\mathbf{y}' \bmod Dq\rangle$ in the first register. Then the residual state can be written by dropping $\mathbf{y}=\mathbf{y}'-\mathbf{v} \bmod Dq$ in Eqn. (17):

$$\begin{aligned}|\varphi_1\rangle &:= \sum_{\mathbf{v}\in L\cap\mathbb{Z}^n_{Dq},\mathbf{v}-\mathbf{y}' \bmod Dq\in\mathbb{Z}^n\cap(r\log n)\mathcal{B}^n_\infty} \exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)\|\mathbf{y}'-\mathbf{v} \bmod Dq\|^2\right)\left|\mathbf{v}-\mathbf{y}' \bmod Dq\right\rangle \\ &= \sum_{\mathbf{v}\in L\cap(\mathbf{y}'+(r\log n)\mathcal{B}^n_\infty)} \exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)\|\mathbf{y}'-\mathbf{v}\|^2\right)\left|\mathbf{v}-\mathbf{y}'\right\rangle.\end{aligned}$$

Here we can change the support in the second line because we set $Dq > \frac{Dq}{\log^2 n} > 4(r\log n)$ (**C.4**), and for $\mathbf{y}'\in\mathbb{Z}^n_{Dq}$, represented as $\mathbf{y}'\in((-Dq/2, Dq/2]\cap\mathbb{Z})^n$, any $\mathbf{v}\in L\cap\mathbb{Z}^n_{Dq}$ such that $\mathbf{v}-\mathbf{y}' \bmod Dq \in \mathbb{Z}^n\cap(r\log n)\mathcal{B}^n_\infty$ can be represented by $\mathbf{v}\in L\cap(\mathbf{y}'+(r\log n)\mathcal{B}^n_\infty)$, i.e., there is no need to wrap around mod Dq.

For the analysis of the next few steps, we write $\mathbf{y}'$ as $\mathbf{y}'=\mathbf{v}+\mathbf{y}$ where $\mathbf{v}\in L$, $\mathbf{y}\in\mathbb{Z}^n\cap r\log n\mathcal{B}^n_\infty$ (here the equation holds over $\mathbb{Z}^n$, not over $\mathbb{Z}^n_{Dq}$, which will be important for the use of $\mathbf{y}'$ in later steps because we will add or subtract $\mathbf{y}'$ over possibly different moduli than Dq; it is possible to write $\mathbf{y}'=\mathbf{v}+\mathbf{y}$ where $\mathbf{v}\in L$, $\mathbf{y}\in\mathbb{Z}^n\cap r\log n\mathcal{B}^n_\infty$ since $Dq\mathbb{Z}^n\in L$, so $\mathbf{y}'\in\mathbf{v}+\mathbf{y}+Dq\mathbb{Z}^n$ and "$+Dq\mathbb{Z}^n$" can be pushed into $\mathbf{v}\in L$). Note that we are not able to efficiently compute such a pair of $\mathbf{v}$, $\mathbf{y}$ from $\mathbf{y}'$ at this moment since finding such a pair requires solving an approximate closest vector problem. We just use $\mathbf{v}$, $\mathbf{y}$ as unknown variables in the analysis of our algorithm. Note that there are multiple pairs of $\mathbf{v}$, $\mathbf{y}$ that satisfy $\mathbf{y}'=\mathbf{v}+\mathbf{y}$, $\mathbf{v}\in L$, $\mathbf{y}\in\mathbb{Z}^n\cap r\log n\mathcal{B}^n_\infty$, we just pick one pair of them (the result of the upcoming analysis is independent of which pair we pick).

Since $\lambda^\infty_2(L) > r\log n > \lambda_1(L)$, $|\varphi_1\rangle$ equals to

$$|\varphi_1\rangle = \sum_{k\in\mathbb{Z},k\mathbf{x}-\mathbf{y}\in(r\log n)\mathcal{B}^n_\infty} \exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)\|k\mathbf{x}-\mathbf{y}\|^2\right)|k\mathbf{x}-\mathbf{y}\rangle.$$

□

For the convenience of Step 2, we show $|\varphi_1\rangle$ is negligibly close to the following state

$$|\varphi'_1\rangle := \sum_{k\in\mathbb{Z}} \exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)\|k\mathbf{x}-\mathbf{y}\|^2\right)|k\mathbf{x}-\mathbf{y} \bmod P\rangle$$

Lemma 3.10. $|\varphi'_1\rangle \approx_t |\varphi_1\rangle$.

Proof. We treat $|\varphi'_1\rangle$, $|\varphi_1\rangle$ as unnormalized vectors over $\mathbb{C}^{nP}$. We have $\||\varphi_1\rangle\|_2^2 \le 2r\log n \in \mathrm{poly}(n)$

since there are at most $2r \log n$ entries in the support. Also,

$$\begin{aligned}\left\| |\varphi_1'\rangle - |\varphi_1\rangle \right\|_1 \leq & \sum_{k\in\mathbb{Z}, k\mathbf{x}-\mathbf{y}\notin (r\log n)\mathcal{B}_\infty^n} \exp\left(-\pi \frac{\|k\mathbf{x}-\mathbf{y}\|^2}{r^2}\right) \\ \in_{Lemma\ 2.6} & \sum_{k\in\mathbb{Z}} \exp\left(-\pi \frac{\|k\mathbf{x}-\mathbf{y}\|^2}{r^2}\right) \cdot \mathrm{negl}(n) \in 2r \cdot \mathrm{negl}(n) \in \mathrm{negl}(n).\end{aligned}$$

Therefore, $\| |\varphi_1'\rangle - |\varphi_1\rangle \|_2 \leq \| |\varphi_1'\rangle - |\varphi_1\rangle \|_1 \in \mathrm{negl}(n) \cdot \| |\varphi_1\rangle \|_2$. So Lemma 3.10 follows Lemma 2.11. □

3.5.2 Step 2: Apply $\mathsf{QFT}_{\mathbb{Z}_P^n}$ on $|\varphi_1\rangle$

In Step 2, we apply $\mathsf{QFT}_{\mathbb{Z}_P^n}$ on $|\varphi_1\rangle$ and get $|\varphi_2\rangle := \mathsf{QFT}_{\mathbb{Z}_P^n} |\varphi_1\rangle$.
The expression of $|\varphi_2\rangle$ is derived as follows:

$$\begin{aligned}|\varphi_2\rangle \approx_t & \sum_{\mathbf{z}\in\mathbb{Z}_P^n} \sum_{k\in\mathbb{Z}} \exp\left(-\pi \left(\frac{s^2+r^2 i}{s^2 r^2}\right) \|k\mathbf{x}-\mathbf{y}\|^2\right) e^{-2\pi i \left\langle k\mathbf{x}-\mathbf{y}, \frac{\mathbf{z}}{P}\right\rangle} |\mathbf{z}\rangle \\ = & \sum_{\mathbf{z}\in\mathbb{Z}_P^n} \sum_{k\in\mathbb{Z}} \exp\left(-\pi \left(\frac{s^2+r^2 i}{s^2 r^2}\right) (k^2\|\mathbf{x}\|^2 - 2k\langle \mathbf{x}, \mathbf{y}\rangle + \|\mathbf{y}\|^2)\right) e^{-2\pi i \left\langle k\mathbf{x}-\mathbf{y}, \frac{\mathbf{z}}{P}\right\rangle} |\mathbf{z}\rangle \\ \propto_{(a)} & \sum_{\mathbf{z}\in\mathbb{Z}_P^n} \sum_{k\in\mathbb{Z}} \exp\left(-\pi \frac{\|\mathbf{x}\|^2(s^2+r^2 i)}{s^2 r^2} \left(k - \frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)^2\right) e^{-2\pi i \left\langle k\mathbf{x}, \frac{\mathbf{z}}{P}\right\rangle} e^{2\pi i \left\langle \mathbf{y}, \frac{\mathbf{z}}{P}\right\rangle} |\mathbf{z}\rangle \\ =_{(b)} & \sum_{\mathbf{z}\in\mathbb{Z}_P^n} \sum_{j\in\mathbb{Z}} \exp\left(-\pi \frac{s^2 r^2 (s^2-r^2 i)}{\|\mathbf{x}\|^2 (s^4+r^4)} \left(j + \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P}\right)^2\right) e^{-2\pi i \frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{x}\|^2} \left(j + \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P}\right)} e^{2\pi i \left\langle \mathbf{y}, \frac{\mathbf{z}}{P}\right\rangle} |\mathbf{z}\rangle,\end{aligned} \tag{18}$$

where $\approx_t$ follows Lemma 3.10; (a) holds since $\exp\left(-\pi \left(\frac{s^2+r^2 i}{s^2 r^2}\right) \|\mathbf{y}\|^2\right)$ and $\exp\left(-\pi \frac{\|\mathbf{x}\|^2(s^2+r^2 i)}{s^2 r^2} \left(\frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)^2\right)$ only contribute to global amplitudes so that can dropped (recall that $\mathbf{x}$ and $\mathbf{y}$ are fixed); (b) uses PSF (Lemma 2.4) and the Fourier transformation of complex Gaussian (Eqn. (1)).

3.5.3 Step 3: Apply a complex Gaussian window on $|\varphi_2\rangle$, get $|\varphi_3\rangle$ and $\mathbf{z}'$

Let us denote $f_2 : \mathbb{Z}^n \mapsto \mathbb{C}$ as the amplitude of $|\mathbf{z}\rangle$ in $|\varphi_2\rangle$, i.e., $|\varphi_2\rangle = \sum_{\mathbf{z}\in\mathbb{Z}_P^n} f_2(\mathbf{z}) |\mathbf{z}\rangle$. Note that we can naturally define f_2 over all $\mathbb{Z}^n$, not just $\mathbb{Z}_P^n$, as $f_2(\mathbf{z}) = f_2(\mathbf{z} \bmod P)$. Setting the domain of f_2 to be $\mathbb{Z}^n$ will be useful in the proof of Lemma 3.20.

In Step 3, we first prepare the following complex Gaussian state using Lemma 2.15: (recall from Cond. **C.6** that V is defined to be $\frac{Pu\sqrt{r^4+s^4}}{rs^2 t}$, the width of the real part of the following state)

$$|\varphi_G\rangle := \sum_{\mathbf{z}_G\in\mathbb{Z}^n \cap V\log n \mathcal{B}_\infty^n} \exp\left(-\pi \frac{t^2 r^2 s^2 (s^2-r^2 i)}{P^2 u^2 (s^4+r^4)} \|\mathbf{z}_G\|^2\right) |\mathbf{z}_G\rangle. \tag{19}$$

We then append $|\varphi_G\rangle$ after $|\varphi_2\rangle$, and add the first register onto the second register:

$$\begin{aligned}|\varphi_2\rangle \otimes |\varphi_G\rangle = &\sum_{\mathbf{z}\in\mathbb{Z}_P^n} f_2(\mathbf{z})\,|\mathbf{z}\rangle \sum_{\mathbf{z}_G\in\mathbb{Z}^n\cap V\log n\mathcal{B}_\infty^n} \exp\left(-\pi\frac{t^2r^2s^2(s^2-r^2i)}{P^2u^2(s^4+r^4)}\|\mathbf{z}_G\|^2\right)|\mathbf{z}_G\rangle \\ \mapsto &\sum_{\mathbf{z}\in\mathbb{Z}_P^n} f_2(\mathbf{z})\,|\mathbf{z}\rangle \sum_{\mathbf{z}_G\in\mathbb{Z}^n\cap V\log n\mathcal{B}_\infty^n} \exp\left(-\pi\frac{t^2r^2s^2(s^2-r^2i)}{P^2u^2(s^4+r^4)}\|\mathbf{z}_G\|^2\right)|\mathbf{z}+\mathbf{z}_G \bmod P\rangle\,.\end{aligned} \tag{20}$$

We now measure the register $|\mathbf{z}+\mathbf{z}_G \bmod P\rangle$ and denote the measurement result as $\mathbf{z}'\in\mathbb{Z}_P^n$. Then the residual state can be written by dropping $\mathbf{z}_G = \mathbf{z}'-\mathbf{z} \bmod P$ into Eqn. (20):

$$\begin{aligned}&\sum_{\mathbf{z}\in\mathbb{Z}_P^n,\mathbf{z}-\mathbf{z}' \bmod P\in\mathbb{Z}^n\cap V\log n\mathcal{B}_\infty^n} f_2(\mathbf{z})\exp\left(-\pi\frac{t^2r^2s^2(s^2-r^2i)}{P^2u^2(s^4+r^4)}\|\mathbf{z}-\mathbf{z}' \bmod P\|^2\right)|\mathbf{z}\rangle \\ =&\sum_{\mathbf{z}\in\mathbf{z}'+(\mathbb{Z}^n\cap V\log n\mathcal{B}_\infty^n)} f_2(\mathbf{z})\exp\left(-\pi\frac{t^2r^2s^2(s^2-r^2i)}{P^2u^2(s^4+r^4)}\|\mathbf{z}-\mathbf{z}'\|^2\right)|\mathbf{z}\rangle =: \left|\varphi_3'\right\rangle \\ \approx_t &\sum_{\mathbf{z}\in\mathbb{Z}^n} f_2(\mathbf{z})\exp\left(-\pi\frac{t^2r^2s^2(s^2-r^2i)}{P^2u^2(s^4+r^4)}\|\mathbf{z}-\mathbf{z}'\|^2\right)|\mathbf{z} \bmod P\rangle =: |\varphi_3\rangle\,.\end{aligned} \tag{21}$$

Here in $=$ we can remove mod P since the support of $\mathbf{z}$ is restricted in $\mathbf{z}'+(\mathbb{Z}^n\cap V\log n\mathcal{B}_\infty^n)$, and $\frac{P}{V} > 2\log n$ (**C.6**), so there is no need to wrap around mod P; $\approx_t$ is proven in Lemma 3.20 in §3.6.2.

From now on we will always assume our guess of $u^2 = \|\mathbf{x}\|^2$ is correct, then

$$\begin{aligned}|\varphi_3\rangle = &\sum_{\mathbf{z}\in\mathbb{Z}^n}\sum_{j\in\mathbb{Z}}\exp\left(-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\left(Pj+\langle\mathbf{x},\mathbf{z}\rangle\right)^2\right)\exp\left(-\pi\frac{t^2r^2s^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\|\mathbf{z}-\mathbf{z}'\|^2\right) \\ &\cdot e^{-2\pi i\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\left(j+\frac{\langle\mathbf{x},\mathbf{z}\rangle}{P}\right)}e^{2\pi i\langle\mathbf{y},\frac{\mathbf{z}}{P}\rangle}\,|\mathbf{z} \bmod P\rangle \\ =_{(a)}\ &\sum_{\mathbf{z}\in\mathbb{Z}^n}\sum_{j\in\mathbb{Z}}\exp\left(-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\left((\mathbf{z}-\mathbf{d}_j)^T\Sigma^{-1}(\mathbf{z}-\mathbf{d}_j)+C_j\right)^2\right) \\ &\cdot e^{-2\pi i\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}j}e^{-2\pi i\left\langle\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2P}-\frac{\mathbf{y}}{P},\mathbf{z}\right\rangle}\,|\mathbf{z} \bmod P\rangle\,,\end{aligned} \tag{22}$$

where

$$\begin{aligned}\mathbf{d}_j := \mathbf{z}' - \mathbf{x}\frac{Pj+\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\quad C_j := \frac{t^2}{t^2+\|\mathbf{x}\|^2}(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)^2, \\ \Sigma^{-1} := t^2\mathbf{I}_n + \mathbf{x}\mathbf{x}^T,\quad \Sigma =_{(b)} \frac{1}{t^2}\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{t^2+\|\mathbf{x}\|^2}\right);\end{aligned} \tag{23}$$

(a) will be proved in Lemma 3.21 in §3.6.2, (b) is derived from Formula (8).

3.5.4 Step 4: Apply $\mathsf{QFT}_{\mathbb{Z}_P^n}$ on $|\varphi_3\rangle$

We compute $|\varphi_4\rangle := \mathsf{QFT}_{\mathbb{Z}_P^n}|\varphi_3\rangle$, which gives

$$
\begin{aligned}
|\varphi_4\rangle &= \sum_{\mathbf{h}\in\mathbb{Z}_P^n}\sum_{\mathbf{z}\in\mathbb{Z}^n}\sum_{j\in\mathbb{Z}} \exp\left(-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\left((\mathbf{z}-\mathbf{d}_j)^T\Sigma^{-1}(\mathbf{z}-\mathbf{d}_j)+C_j\right)^2\right) e^{-2\pi i\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}j} e^{-2\pi i\left\langle\frac{\mathbf{h}}{P}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2P}-\frac{\mathbf{y}}{P},\mathbf{z}\right\rangle}|\mathbf{h}\rangle \\
&=_{(a)} \sum_{\mathbf{h}\in\mathbb{Z}_P^n}\sum_{\mathbf{m}\in\mathbb{Z}^n} \exp\left(-\pi\frac{P^2\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{m}+\frac{\mathbf{h}}{P}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2P}-\frac{\mathbf{y}}{P}\right)^T\cdot\Sigma\cdot\left(\mathbf{m}+\frac{\mathbf{h}}{P}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2P}-\frac{\mathbf{y}}{P}\right)\right) \\
&\qquad\cdot\sum_{j\in\mathbb{Z}} e^{-2\pi i\left\langle\mathbf{d}_j,\mathbf{m}+\frac{\mathbf{h}}{P}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2P}-\frac{\mathbf{y}}{P}\right\rangle}\cdot e^{-2\pi i\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}j}\cdot e^{-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}C_j}|\mathbf{h}\rangle \\
&= \sum_{\mathbf{h}\in\mathbb{Z}_P^n}\sum_{\mathbf{m}\in P\mathbb{Z}^n} \exp\left(-\pi\frac{\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)^T\cdot\Sigma\cdot\left(\mathbf{h}+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)\right) \\
&\qquad\cdot\sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{\left\langle\mathbf{d}_j,\mathbf{h}+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right\rangle}{P}}\cdot e^{-2\pi i\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}j}\cdot e^{-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}C_j}|\mathbf{h}\rangle,
\end{aligned}
\tag{24}
$$

where $\Sigma^{-1},\Sigma,\mathbf{d}_j,C_j$ are defined in Eqn. (23); (a) uses PSF from $\sum_{\mathbf{z}\in\mathbb{Z}^n}$ to $\sum_{\mathbf{m}\in\mathbb{Z}^n}$.

3.5.5 Step 5: Split $|\varphi_4\rangle$ into higher and lower order bits $|\mathbf{h}'\rangle|\mathbf{h}''\rangle$, then measure $|\mathbf{h}''\rangle$

Recall from Condition **C.2** that $M=\frac{P}{t^2+u^2}$. We write the variable $\mathbf{h}$ in $|\varphi_4\rangle$ as $\mathbf{h}=\mathbf{h}'\cdot(t^2+u^2)+\mathbf{h}''$, where $\mathbf{h}'\in\mathbb{Z}_M^n$ represents the higher order bits of $\mathbf{h}$, and $\mathbf{h}''\in\mathbb{Z}_{t^2+u^2}^n$ represents the lower order bits of $\mathbf{h}$. Therefore $|\mathbf{h}\rangle$ can be split into $|\mathbf{h}'\rangle|\mathbf{h}''\rangle$. We then measure the $|\mathbf{h}''\rangle$ register and denote the measurement result as $\mathbf{h}^*\in\mathbb{Z}_{t^2+u^2}^n$, denote the residual state as $|\varphi_5\rangle$.

To derive the expression of $|\varphi_5\rangle$, we note that $|\varphi_4\rangle$ can be equivalently written as

$$
\begin{aligned}
|\varphi_4\rangle = \sum_{\mathbf{h}'\in\mathbb{Z}_M^n}\sum_{\mathbf{h}''\in\mathbb{Z}_{t^2+\|\mathbf{x}\|^2}^n}\sum_{\mathbf{m}\in P\mathbb{Z}^n} & e^{-\pi\frac{\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}''+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)^T\cdot\Sigma\cdot\left(\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}''+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)} \\
&\cdot\sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{\left\langle\mathbf{z}'-\mathbf{x}\frac{Pj+\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}''+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right\rangle}{P}}\cdot e^{-2\pi i\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}j}\cdot e^{-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}C_j}\left|\mathbf{h}'\right\rangle\left|\mathbf{h}''\right\rangle.
\end{aligned}
\tag{25}
$$

We then measure the $|\mathbf{h}''\rangle$ register and denote the result as $\mathbf{h}^*\in\mathbb{Z}_{t^2+\|\mathbf{x}\|^2}^n$. In Lemma 3.24 in §3.6.3, we show that, with probability $1-2^{-\Omega(n)}$ over the randomness in the measurement, $\mathbf{h}^*$ satisfies $\mathrm{dist}\left(\frac{\langle\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}+\frac{\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\mathbb{Z}\right)\le\frac{2ut^2}{r}\sqrt{n}\log n <_{\mathbf{C.7}}\frac{1}{4\beta\log n}$.

To understand how $|\varphi_5\rangle$ looks like, let us take a closer look at the term inside $\sum_{j\in\mathbb{Z}}$ in Eqn. (25). In

fact, the only term that depends on all $\mathbf{h}'$, $\mathbf{m}$, and j is

$$\begin{aligned} e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{Pj+\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}^*+\mathbf{m}}{P}\right\rangle} &= e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{Pj+\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'+\frac{\mathbf{h}^*+\mathbf{m}}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle} \\ &= e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'+\frac{\mathbf{h}^*+\mathbf{m}}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle}\cdot e^{-2\pi i\left\langle -\mathbf{x}\frac{Pj}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'+\frac{\mathbf{h}^*+\mathbf{m}}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle} \\ &= e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'+\frac{\mathbf{h}^*+\mathbf{m}}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle}\cdot e^{2\pi i\left\langle \mathbf{x}j,\mathbf{h}'+\frac{\mathbf{h}^*+\mathbf{m}}{t^2+\|\mathbf{x}\|^2}\right\rangle} \end{aligned}$$

Since $\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}\in\mathbb{Z}^n$, $\mathbf{x}\in\mathbb{Z}^n$, $j\in\mathbb{Z}$, so $e^{2\pi i\left\langle \mathbf{x}j,\mathbf{h}'+\frac{\mathbf{h}^*+\mathbf{m}}{t^2+\|\mathbf{x}\|^2}\right\rangle}=e^{2\pi i\left\langle \mathbf{x}j,\frac{\mathbf{h}^*}{t^2+\|\mathbf{x}\|^2}\right\rangle}$. Therefore, the term $\sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{\left\langle -\mathbf{x}\frac{Pj}{t^2+\|\mathbf{x}\|^2},\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}''+\mathbf{m}+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right\rangle}{P}}\cdot e^{-2\pi i\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}j}\cdot e^{-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}C_j}$ in Eqn. (25) is completely independent of $\mathbf{h}'$, $\mathbf{m}$, i.e., it merely contributes to the global amplitude of $|\varphi_5\rangle$. So

$$\begin{aligned} |\varphi_5\rangle = \sum_{\mathbf{h}'\in\mathbb{Z}_M^n}\sum_{\mathbf{m}\in P\mathbb{Z}^n} & e^{-\pi\frac{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)^T\cdot\Sigma\cdot\left(\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)} \\ & \cdot e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'+\frac{\mathbf{m}+\mathbf{h}^*}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle}\left|\mathbf{h}'\right\rangle. \end{aligned} \tag{26}$$

3.5.6 Step 6: Apply $\mathsf{QFT}_{\mathbb{Z}_M^n}$ on $|\varphi_5\rangle$

We compute $|\varphi_6\rangle := \mathsf{QFT}_{\mathbb{Z}_M^n}|\varphi_5\rangle$. Recall from Cond. **C.6** where we define $\sigma=\frac{rs^2t}{u\sqrt{r^4+s^4}}\in\left(2\log n,\frac{D}{4\log n}\right)$, an important width parameter used in Steps 6 and 7. We show in Lemmas 3.27 and 3.29 in §3.6.4 that $|\varphi_6\rangle$ is negl(n)-close to (we remove the support in $|\varphi_6\rangle$ with negligible weight to get $|\varphi_6'''\rangle$):

$$\begin{aligned} \left|\varphi_6'''\right\rangle = \sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1},\ j\in\mathbb{Z}\text{ s.t.}\\ \left\|\frac{M}{2}\mathbf{k_c}-(\mathbf{z}'+\mathbf{h}^*-\mathbf{y})-\mathbf{x}\langle \mathbf{x},\mathbf{k_c}\rangle+2Dj\mathbf{x}+\mathbf{x}\left(\frac{\langle \mathbf{z}'+\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{\langle \mathbf{y},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)-\mathbf{c}\right\|_\infty\le\sigma\log n}} & e^{-\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right)\right\|^2}{\sigma^2}} \\ & \cdot e^{-\pi\frac{1}{\sigma_x^2}\left\|2Dj\mathbf{x}-\left(\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\mathbf{x}\right\|^2}\cdot e^{2\pi i\phi_6(\mathbf{c},\mathbf{k_c},j)}\left|\mathbf{c}\right\rangle, \end{aligned} \tag{27}$$

where $\mathbf{c}':=\mathbf{c}+\mathbf{z}'+\mathbf{h}^*-\mathbf{y}+\mathbf{x}\left(\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)$, $\sigma_x^2\in\mathbb{C}$ satisfies $Re\left(\frac{1}{\sigma_x^2}\right)\in\frac{1}{\sigma^2}\cdot(1,3)$, $\phi_6(\mathbf{c},\mathbf{k_c},j)\in\mathbb{R}$ contains phase terms:

$$\begin{aligned} e^{2\pi i\phi_6(\mathbf{c},\mathbf{k_c},j)} := {} & e^{2\pi i\mathbf{k_c}^T\cdot\frac{\mathbf{c}+\mathbf{z}'-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}}{M}}\cdot e^{-2\pi i\frac{\left\|\mathbf{c}+\mathbf{z}'-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}\right\|^2}{M^2}} \\ & \cdot e^{-2\pi i\left(\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{M\|\mathbf{x}\|^2}\left(2Dj-\left(\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)+\frac{t^2}{M^2}\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle^2}{\|\mathbf{x}\|^4}\right)}. \end{aligned} \tag{28}$$

$|\varphi_6\rangle$ is an important state in the whole algorithm, but its detailed proofs are long – the proof of Lemma 3.27 (the Fourier transform calculation for $|\varphi_6\rangle$) alone takes about seven pages, so we defer them to §3.6.4. Here let us provide some explanations about $|\varphi_6'''\rangle$. For $|\varphi_6'''\rangle$, its support contains $2^{n-1}\cdot\frac{M}{2D^2}$ elliptical Gaussian balls (see Figure 2-(f)), centered at

$$\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})-\mathbf{x}\langle\mathbf{x},\mathbf{k_c}\rangle+2Dj\mathbf{x}+\mathbf{x}\left(\frac{\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{\langle\mathbf{y},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right), \tag{29}$$

for some $\mathbf{k_c}\in 0|\mathbb{Z}^{n-1}$ and $j\in\mathbb{Z}$ (formally proved in Lemma 3.28). The width of the elliptical Gaussian balls is σ in the direction orthogonal to $\mathbf{x}$, and is slightly smaller than σ in the direction of $\mathbf{x}$. The width σ is smaller than $\frac{D}{4\log n}$, indicating that Karst wave appears, and we will use rounding to $D\mathbb{Z}^n$ to extract the centers of those Gaussian balls in Step 7. Note that $\mathbf{k_c}$ runs over $0|\mathbb{Z}^{n-1}$ instead of $\mathbb{Z}^n$ since we decompose the support into those on the same line with $\mathbf{b}=\frac{\mathbf{x}}{D}$ (running over $j\in\mathbb{Z}$) and those not on the same line with $\mathbf{b}$ (running over $\mathbf{k_c}\in 0|\mathbb{Z}^{n-1}$), and there is a simple bijection between $\mathbb{Z}^n$ and $0|\mathbb{Z}^{n-1}\times\mathbf{b}\mathbb{Z}$, since we know the first coordinate of $\mathbf{b}$ is -1.

3.5.7 Step 7: Extract the centers of $|\varphi_6\rangle$ to get a purely imaginary Gaussian state $|\varphi_7\rangle$

Recall from Eqn. (27) that $|\varphi_6'''\rangle$ can be written as

$$\begin{aligned}|\varphi_6'''\rangle = \sum_{\substack{\mathbf{c}\in\mathbb{Z}^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1},\ j\in\mathbb{Z}\text{ s.t.}\\ \left\|\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})-\mathbf{x}\langle\mathbf{x},\mathbf{k_c}\rangle+2Dj\mathbf{x}+\mathbf{x}\left(\frac{\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{\langle\mathbf{y},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)-\mathbf{c}\right\|_\infty\le\sigma\log n}} e^{-\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right)\right\|^2}{\sigma^2}}\\ \cdot e^{-\pi\frac{1}{\sigma_x^2}\left\|2Dj\mathbf{x}-\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\mathbf{x}\right\|^2}\cdot e^{2\pi i\phi_6(\mathbf{c},\mathbf{k_c},j)}\,|\mathbf{c}\bmod M\rangle,\end{aligned}$$

where

$$\begin{aligned}e^{2\pi i\phi_6(\mathbf{c},\mathbf{k_c},j)} &:= e^{2\pi i\mathbf{k_c}^T\cdot\frac{\mathbf{c}+\mathbf{z'}-\frac{\langle\mathbf{x},\mathbf{z'}\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}}{M}}\cdot e^{-2\pi i\frac{\left\|\mathbf{c}+\mathbf{z'}-\frac{\langle\mathbf{x},\mathbf{z'}\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}\right\|^2}{M^2}}\\ &\quad\cdot e^{-2\pi i\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{M\|\mathbf{x}\|^2}\left(2Dj-\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)+\frac{t^2}{M^2}\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle^2}{\|\mathbf{x}\|^4}\right)}\\ &= \underbrace{e^{-2\pi i\frac{\left\|\mathbf{c}+\mathbf{z'}-\frac{\langle\mathbf{x},\mathbf{z'}\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}-\frac{M}{2}\mathbf{k_c}\right\|^2}{M^2}}}_{=:I_1}\cdot e^{2\pi i\frac{\|\mathbf{k_c}\|^2}{4}}\\ &\quad\cdot\underbrace{e^{-2\pi i\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{M\|\mathbf{x}\|^2}\left(2Dj-\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)}}_{=:I_2}\cdot\underbrace{e^{-2\pi i\frac{t^2}{M^2}\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle^2}{\|\mathbf{x}\|^4}}}_{=:I_3}.\end{aligned} \tag{30}$$

Here we regroup the exponents in the second line for the convenience of the upcoming calculations.

Let us remark that here we write $|\varphi_6'''\rangle=\sum_{\mathbf{c}\in\mathbb{Z}^n}f_6(\mathbf{c})\,|\mathbf{c}\bmod M\rangle$ instead of $|\varphi_6'''\rangle=\sum_{\mathbf{c}\in\mathbb{Z}_M^n}f_6(\mathbf{c})\,|\mathbf{c}\rangle$ in Eqn. (27). We can do so because the amplitude function f_6 is M-periodic. To see why, recall that

$|\varphi_6\rangle = \mathsf{QFT}_{\mathbb{Z}_M^n} |\varphi_5\rangle$, and we derive the amplitudes in Eqn. (27) without using the fact that $\mathbf{c} \in \mathbb{Z}_M^n$, so that the expression of $f_6(\mathbf{c})$ directly holds for all $\mathbf{c} \in \mathbb{Z}^n$ and is M-periodic.

In Step 7 we perform four operations. The main purpose of those operations is to extract the centers of Gaussian balls in $|\varphi_6\rangle$ to get a state where the amplitude is purely imaginary Gaussian.

Lemma 3.11. *There is a quantum algorithm that takes as input $|\varphi_6'''\rangle$, $\mathbf{y}'$, $\mathbf{z}'$, $\mathbf{h}^*$, outputs a state*

$$|\varphi_7\rangle := \sum_{\mathbf{k_c} \in 0|\mathbb{Z}^{n-1}, j \in \mathbb{Z}} e^{-2\pi i \frac{(2Dj - \langle \mathbf{k_c}, \mathbf{x} \rangle)^2}{2M}} e^{2\pi i \frac{\|\mathbf{k_c}\|^2}{4}} \left| (2Dj - \langle \mathbf{k_c}, \mathbf{x} \rangle)\mathbf{x} + k'\mathbf{x} - \mathbf{v} + \frac{M}{2}\mathbf{k_c} \bmod M \right\rangle,$$

where $k' := \left\lfloor \left(\frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} \right) \right\rceil$. The running time is in $\mathrm{poly}(n)$.

Proof. The first operation takes the register from $|\mathbf{c} \bmod M\rangle$ to $|\mathbf{c} + \mathbf{z}' + \mathbf{h}^* - \mathbf{y}' \bmod M\rangle$. Note that $\mathbf{y}' \in \mathbb{Z}_{Dq}^n$ is obtained in Step 1, $\mathbf{z}' \in \mathbb{Z}_P^n$ is obtained in Step 3, $\mathbf{h}^* \in \mathbb{Z}_{\frac{M}{2}}^n$ is obtained in Step 5, so we can perform this operation efficiently. Here we interpret $\mathbf{y}'$, $\mathbf{z}'$, $\mathbf{h}^*$ as strings in $\mathbb{Z}^n$. Readers may worry that the modulus of $\mathbf{y}' \in \mathbb{Z}_{Dq}^n$ and $\mathbf{h}^* \in \mathbb{Z}_{\frac{M}{2}}^n$ does not divide M, and it may cause a problem later. Here we will guarantee that the modulus does not cause a problem because the main equation for representing the centers of Gaussian balls, Eqn. (29), holds over $\mathbb{Z}^n$, and recall in Step 1 that we can write $\mathbf{y}' = \mathbf{v} + \mathbf{y}$ where the equation also holds over $\mathbb{Z}^n$.

Let us move on. The second operation computes the following in the second register:

$$\begin{aligned} \lfloor \mathbf{c} + \mathbf{z}' + \mathbf{h}^* - \mathbf{y}' \bmod M \rceil_D &\in_{(a)} \left\lfloor \frac{M}{2}\mathbf{k_c} - \mathbf{x}\langle \mathbf{x}, \mathbf{k_c} \rangle + 2Dj\mathbf{x} + \mathbf{x}\left(\frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} \right) - \mathbf{v} + \sigma \log n \mathcal{B}_\infty^n \bmod M \right\rceil_D \\ &=_{(b)} \frac{M}{2}\mathbf{k_c} - \mathbf{x}\langle \mathbf{x}, \mathbf{k_c} \rangle + 2Dj\mathbf{x} + \mathbf{x}\left\lfloor \frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} \right\rceil - \mathbf{v} \bmod M, \end{aligned} \tag{31}$$

where (a) is derived from the formula of the centers of $\mathbf{c}$ in Eqn. (29); (b) is derived from $\sigma \log n < \frac{D}{4}$ (**C.6**), and the fact that $\frac{M}{2}\mathbf{k_c} - \mathbf{x}\langle \mathbf{x}, \mathbf{k_c} \rangle + 2Dj\mathbf{x} - \mathbf{v} \in D\mathbb{Z}^n$, and the following equation:

$$\mathbf{x}\left(\frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} \right) =_{(c)} \mathbf{x}\left\lfloor \frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} \right\rceil + \mathbf{x}e \in_{(d)} \mathbf{x}\left\lfloor \frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} \right\rceil + \frac{D}{4}\mathcal{B}_\infty^n,$$

where (c) uses Lemma 3.24 which implies $\frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} = \left\lfloor \frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} \right\rceil + e$ where $|e| \leq \frac{2ut^2}{r}\sqrt{n}\log n \leq_{\mathbf{C.7}} \frac{1}{4\beta \log n}$; (d) uses $\|\mathbf{b}\|_\infty \leq \beta \log n$ in Lemma 3.6. Therefore Eqn. (31) holds.

From now on we denote $k' := \left\lfloor \left(\frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} \right) \right\rceil$. So after two operations, we get $|\varphi_{6.b}\rangle$:

$$\begin{aligned} |\varphi_{6.b}\rangle := \sum_{\substack{\mathbf{c} \in \mathbb{Z}^n,\ \mathbf{k_c} \in 0|\mathbb{Z}^{n-1},\ j \in \mathbb{Z} \text{ s.t.} \\ \left\| \frac{M}{2}\mathbf{k_c} - (\mathbf{z}' + \mathbf{h}^* - \mathbf{y}) - \mathbf{x}\langle \mathbf{x}, \mathbf{k_c} \rangle + 2Dj\mathbf{x} + \mathbf{x}\left(\frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x} \rangle}{t^2 + \|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x} \rangle}{\|\mathbf{x}\|^2} \right) - \mathbf{c} \right\|_\infty \leq \sigma \log n}} & e^{-\pi \frac{\left\| \left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2} \right)\left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c} \right) \right\|^2}{\sigma^2}} \\ & \cdot e^{-\pi \frac{1}{\sigma_x^2} \left\| 2Dj\mathbf{x} - \left(\frac{\left\langle \left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c} \right), \mathbf{x} \right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \mathbf{h}^* - \frac{M}{2}\mathbf{k_c}, \mathbf{x} \right\rangle}{t^2 + \|\mathbf{x}\|^2} \right)\mathbf{x} \right\|^2} \cdot e^{2\pi i \phi_6(\mathbf{c}, \mathbf{k_c}, j)} \\ & \left| \mathbf{c} + \mathbf{z}' + \mathbf{h}^* - \mathbf{y}' \bmod M \right\rangle \left| \frac{M}{2}\mathbf{k_c} + \left(2Dj - \langle \mathbf{k_c}, \mathbf{x} \rangle + k' \right)\mathbf{x} - \mathbf{v} \bmod M \right\rangle. \end{aligned} \tag{32}$$

In the third operation, we subtract (over $\mathbb{Z}_M^n$) the first register by the second register and denote the result as $|\varphi_{6.c}\rangle$. To derive the expression of $|\varphi_{6.c}\rangle$, we let $\mathbf{d} := \mathbf{c}+\mathbf{z}'+\mathbf{h}^*-\mathbf{y}'-\left(\frac{M}{2}\mathbf{k_c} + (2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle + k')\,\mathbf{x} - \mathbf{v}\right)$. Then we can rewrite the common expressions in Eqn. (32) and Eqn. (30) as

$$\begin{aligned}
\mathbf{c} + \mathbf{z}' - \frac{\langle \mathbf{x}, \mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2} - \frac{M}{2}\mathbf{k_c} =\ & \mathbf{d} - (\mathbf{h}^* - \mathbf{y}') + (2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle + k')\,\mathbf{x} - \mathbf{v} - \frac{\langle \mathbf{x}, \mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2} \\
\frac{\left\langle \left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c}\right), \mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} =\ & 2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle + \frac{\langle \mathbf{d}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{v}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} + k' - \frac{\langle \mathbf{z}', \mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{y}', \mathbf{x}\rangle}{\|\mathbf{x}\|^2} \\
\frac{\left\langle \left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c}\right), \mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \left(\mathbf{h}^* - \frac{M}{2}\mathbf{k_c}\right), \mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2} - 2Dj =\ & \frac{\langle \mathbf{d}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{v}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} + k' - \frac{\langle \mathbf{z}' + \mathbf{h}^*, \mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{y}', \mathbf{x}\rangle}{\|\mathbf{x}\|^2}.
\end{aligned} \tag{33}$$

Therefore $|\varphi_{6.c}\rangle$ equals to

$$\begin{aligned}
|\varphi_{6.c}\rangle := \sum_{\substack{\mathbf{d}\in\mathbb{Z}^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1},\ j\in\mathbb{Z} \text{ s.t.} \\ \left\|\mathbf{x}\left(\frac{\langle \mathbf{z}'+\mathbf{h}^*, \mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} - \frac{\langle \mathbf{y}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} - k'\right) - \mathbf{d}\right\|_\infty \le \sigma \log n}} & e^{-\pi \frac{\left\|\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}} \cdot e^{-\pi \frac{1}{\sigma_x^2}\left\|\left(\frac{\langle \mathbf{d}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} + k' - \frac{\langle \mathbf{z}'+\mathbf{h}^*, \mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{y}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)\mathbf{x}\right\|^2} \\
& \cdot e^{2\pi i \phi_7(\mathbf{d}, \mathbf{k_c}, j)}\, |\mathbf{d}\rangle \left| \frac{M}{2}\mathbf{k_c} + \left(2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle + k'\right)\mathbf{x} - \mathbf{v} \bmod M \right\rangle,
\end{aligned}$$

where $\phi_7(\mathbf{d}, \mathbf{k_c}, j) \in \mathbb{R}$ is the phase term by rewriting $\mathbf{c}$ in $\phi_6(\mathbf{c}, \mathbf{k_c}, j)$ as a function of $\mathbf{d}, \mathbf{k_c}, j$ (the expression will be given soon in Claim 3.12). Note that the real amplitude in the first line of $|\varphi_{6.c}\rangle$ is independent of j and $\mathbf{k_c}$.

After measuring $|\mathbf{d}\rangle \to \mathbf{d}'$ ($\mathbf{d}'$ is not used anymore so we can throw it away), the residual state $|\varphi_7\rangle$ is

$$|\varphi_7\rangle = \sum_{\mathbf{k_c}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{2\pi i \phi_7(\mathbf{d}', \mathbf{k_c}, j)} \left| (2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle)\,\mathbf{x} + \left(k'\mathbf{x} - \mathbf{v}\right) + \frac{M}{2}\mathbf{k_c} \bmod M \right\rangle. \tag{34}$$

Claim 3.12. $e^{2\pi i \phi_7(\mathbf{d}', \mathbf{k_c}, j)} \propto e^{-2\pi i \frac{(2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle)^2}{2M}} e^{2\pi i \frac{\|\mathbf{k_c}\|^2}{4}}$.

Proof. We replace the use of $\mathbf{c}$ in $e^{2\pi i \phi_6(\mathbf{c}, \mathbf{k_c}, j)}$ in Eqn. (30) by $\mathbf{d}$ (see the common replacements in Eqn. (33)). We check each term of I_1, I_2, I_3 carefully (here $\propto$ hides terms that contribute to the constant phase of the state, we will only keep terms that depend on j or $\mathbf{k_c}$):

$$\begin{aligned}
I_1 = I_1(\mathbf{k_c}, j) =\ & e^{-2\pi i \frac{1}{M^2}\|\mathbf{c}+\mathbf{z}' - \frac{\langle \mathbf{x}, \mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2} - \frac{M}{2}\mathbf{k_c}\|^2} = e^{-2\pi i \frac{1}{M^2}\|\mathbf{d} - (\mathbf{h}^* - \mathbf{y}') + (2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle + k')\mathbf{x} - \mathbf{v} - \frac{\langle \mathbf{x}, \mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\|^2} \\
\propto\ & e^{-2\pi i \frac{1}{M^2}\left((2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle)^2\|\mathbf{x}\|^2 + 2(2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle)\cdot \mathbf{x}^T \cdot \left(\mathbf{d} - (\mathbf{h}^* - \mathbf{y}') + k'\mathbf{x} - \mathbf{v} - \frac{\langle \mathbf{x}, \mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)}, \\
I_2 = I_2(\mathbf{k_c}, j) =\ & e^{-2\pi i \left(\frac{\left\langle \left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c}\right), \mathbf{x}\right\rangle}{M\|\mathbf{x}\|^2}\left(2Dj - \left(\frac{\left\langle \left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c}\right), \mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \mathbf{h}^* - \frac{M}{2}\mathbf{k_c}, \mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)\right)} \\
=\ & e^{2\pi i \frac{1}{M}\left(2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle + \frac{\langle \mathbf{d}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{v}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} + k' - \frac{\langle \mathbf{z}', \mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{y}', \mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)\left(\frac{\langle \mathbf{d}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{v}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} + k' - \frac{\langle \mathbf{z}'+\mathbf{h}^*, \mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{y}', \mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)} \\
\propto\ & e^{2\pi i \frac{1}{M}(2Dj - \langle \mathbf{k_c}, \mathbf{x}\rangle)\left(\frac{\langle \mathbf{d}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{v}, \mathbf{x}\rangle}{\|\mathbf{x}\|^2} + k' - \frac{\langle \mathbf{z}'+\mathbf{h}^*, \mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{y}', \mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)},
\end{aligned}$$

$$
\begin{aligned}
I_3 = I_3(\mathbf{k_c}, j) = \; & e^{-2\pi i\left(\frac{t^2}{M^2}\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle^2}{\|\mathbf{x}\|^4}\right)} \\
= \; & e^{-2\pi i\frac{t^2}{M^2}\left(2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle+\frac{\langle\mathbf{d},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}-\frac{\langle\mathbf{v},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}+k'-\frac{\langle\mathbf{z}',\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}+\frac{\langle\mathbf{y}',\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)^2}. \\
\propto \; & e^{-2\pi i\frac{t^2}{M^2}\left((2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle)^2+2(2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle)\left(\frac{\langle\mathbf{d},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}-\frac{\langle\mathbf{v},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}+k'-\frac{\langle\mathbf{z}',\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}+\frac{\langle\mathbf{y}',\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)\right)}.
\end{aligned}
$$

To verify $e^{2\pi i\phi_7(\mathbf{d}',\mathbf{k_c},j)} = I_1\cdot I_2\cdot I_3\cdot e^{2\pi i\frac{\|\mathbf{k_c}\|^2}{4}} = e^{-2\pi i\frac{(2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle)^2}{2M}}e^{2\pi i\frac{\|\mathbf{k_c}\|^2}{4}}$, we check every terms. The terms involving $(2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle)^2$ only appear in I_1 and I_3, where the coefficient is $-\frac{\|\mathbf{x}\|^2}{M^2}-\frac{t^2}{M^2}=-\frac{1}{2M}$. The terms involving $(2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle)\left(\frac{\langle\mathbf{d},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}-\frac{\langle\mathbf{v},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}+k'-\frac{\langle\mathbf{z}',\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}+\frac{\langle\mathbf{y}',\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)$ appear in I_1, I_2, and I_3, where the coefficient is $-\frac{2\|\mathbf{x}\|^2}{M^2}+\frac{1}{M}-\frac{2t^2}{M^2}=0$. The terms involving $(2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle)\left(-\frac{\langle\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}\right)$ appear in I_1 and I_2, where the coefficient is $-\frac{2(t^2+\|\mathbf{x}\|^2)}{M^2}+\frac{1}{M}=0$. This concludes the proof of Claim 3.12. □

This concludes the proof of Lemma 3.11. □

For the convenience of the upcoming analysis, we make a few notation changes in $|\varphi_7\rangle$. First, since $k'\mathbf{x}-\mathbf{v}$ is fixed before the end of Step 7, we combine it in one term by denoting it as $\mathbf{v}' := k'\mathbf{x}-\mathbf{v}$. Second, since we set $\mathbf{b}_{[2\ldots n]}\in 2\mathbb{Z}$, we can make sure that $\langle\mathbf{k_c},\mathbf{x}\rangle\in 2D\mathbb{Z}$ for any $\mathbf{k_c}\in 0\mid\mathbb{Z}^{n-1}$, so we can change the variable $2Dj-\langle\mathbf{k_c},\mathbf{x}\rangle$ to $2Dj'$ for some j' (note that without $\mathbf{b}_{[2\ldots n]}\in 2\mathbb{Z}$, we cannot make such a change; all calculations in previous steps hold even when $\mathbf{b}_{[2\ldots n]}\notin 2\mathbb{Z}$). Therefore $|\varphi_7\rangle$ can be equivalently written as:

$$
\begin{aligned}
|\varphi_7\rangle = & \sum_{\mathbf{k_c}\in 0|\mathbb{Z}^{n-1},j'\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj')^2}{2M}}e^{2\pi i\frac{\|\mathbf{k_c}\|^2}{4}}\left|2Dj'\mathbf{x}+\mathbf{v}'+\frac{M}{2}\mathbf{k_c} \bmod M\right\rangle \\
= & \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1},j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}}e^{2\pi i\frac{\|\mathbf{k}\|^2}{4}}\left|2Dj\mathbf{x}+\mathbf{v}'+\frac{M}{2}\mathbf{k} \bmod M\right\rangle,
\end{aligned}
\tag{35}
$$

where in the second line we keep simplifying notations by changing j' to j and changing $\mathbf{k_c}$ to $\mathbf{k}$ (since now there is no link from $\mathbf{k_c}$ to $\mathbf{c}$, unlike in Steps 6).

3.5.8 Step 8: Extract $v_1' \bmod D^2p_1$ and keep $|\varphi_8\rangle = |\varphi_7\rangle$

In Step 8, we first perform four operations, then make a partial measurement, and finally reverse the four operations (we will make sure that the four operations are reversible). The goal is to extract $v_1' \bmod D^2p_1$, and in the end get back to $|\varphi_7\rangle$. I.e., we will learn $v_1' \bmod D^2p_1$ without collapsing or modifying $|\varphi_7\rangle$.

Lemma 3.13. *There is a* $\mathrm{poly}(n)$ *time quantum algorithm that takes* $|\varphi_7\rangle$ *defined in Eqn.* (35) *as input, outputs* $v_1' \bmod D^2p_1$ *and* $|\varphi_8\rangle = |\varphi_7\rangle$.

Proof. In the first operation, we apply the domain extension trick (Lemma 2.17, which is reversible) to extend the modulus from M to DM, so as to get

$$|\varphi_{7.a}\rangle = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} e^{2\pi i\frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{x}+\mathbf{v}'+\frac{M}{2}\mathbf{k} \bmod DM\right\rangle.$$

In the second operation, we "divide the whole register by D". We can do so because $2Dj\mathbf{x}+\mathbf{v}'+\frac{M}{2}\mathbf{k} \in D\mathbb{Z}^n$, so we simply measure the modulo D part of the register (we will always get $0^n \bmod D$), and interpret the remaining register as being divided by D. So the residual state becomes

$$|\varphi_{7.b}\rangle = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} e^{2\pi i\frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{b}+\frac{\mathbf{v}'}{D}+\frac{M}{2D}\mathbf{k} \bmod M\right\rangle.$$

Note that this operation is also reversible: we just "multiply by D" by creating $|0^n \bmod D\rangle$ and interpreting them as the LSBs.

The third operation applies the phase kickback trick on the first coordinate, $-2Dj+\frac{\mathbf{v}'}{D} \bmod M$, to multiply $e^{2\pi i\frac{((2Dj)\cdot(-1)+\frac{v_1'}{D})^2}{2M}} \propto e^{2\pi i\frac{(2Dj)^2-2(2Dj)\frac{v_1'}{D}}{2M}}$ on the amplitude, so as to remove the quadratic term of j in the amplitude and get

$$|\varphi_{7.c}\rangle = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)\frac{v_1'}{D}}{M}} e^{2\pi i\frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{b}+\frac{\mathbf{v}'}{D}+\frac{M}{2D}\mathbf{k} \bmod M\right\rangle.$$

Let us remark that the first three operations in Step 8 preserve the M-periodicity of the amplitude: the amplitude remains M-periodic after the first two operations; in the third operation, for any $a\in\mathbb{Z}$, $\frac{(a+M)^2}{2M} = \frac{a^2+2aM+M^2}{2M} \in_{M\in 2\mathbb{Z}} \frac{a^2}{2M}+\mathbb{Z}$, so the "mod M" in $-2Dj+\frac{\mathbf{v}'}{D} \bmod M$ can be dropped in $e^{2\pi i\frac{((2Dj)\cdot(-1)+\frac{v_1'}{D})^2}{2M}}$, and the third operation also preserves M-periodicity.

The fourth operation applies $\mathsf{QFT}_{\mathbb{Z}_M^n}$ on $|\varphi_{7.c}\rangle$ and get

$$|\varphi_{7.d}\rangle = \sum_{\mathbf{w}\in\mathbb{Z}_M^n} \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)\left(\langle\mathbf{b},\mathbf{w}\rangle+\frac{v_1'}{D}\right)}{M}} e^{-2\pi i\frac{\left\langle\frac{\mathbf{v}'}{D},\mathbf{w}\right\rangle}{M}} e^{2\pi i\left(\frac{\|\mathbf{k}\|^2}{4}-\frac{\langle\mathbf{k},\mathbf{w}\rangle}{2D}\right)} |\mathbf{w}\rangle.$$

Before we describe the fifth operation, let us first understand what if we measure the entire $|\mathbf{w}\rangle$ now.

Claim 3.14. *If we measure $|\mathbf{w}\rangle$ in $|\varphi_{7.d}\rangle$, then we always get a vector $\mathbf{w}\in\mathbb{Z}_M^n$ that satisfies $\langle\mathbf{b},\mathbf{w}\rangle+\frac{v_1'}{D} \equiv 0 \pmod{\frac{M}{2D}}$, $\mathbf{w}_{[2\ldots n]}\in D\mathbb{Z}^{n-1}$, and $w_1 \equiv \frac{v_1'}{D} \pmod{Dp_1}$.*

Proof. Let us first fix any $\mathbf{k}\in 0 \mid \mathbb{Z}^{n-1}$ and look at the only term in the amplitude of $|\varphi_{7.d}\rangle$ that depends on j: $e^{-2\pi i\frac{(2Dj)\left(\langle\mathbf{b},\mathbf{w}\rangle+\frac{v_1'}{D}\right)}{M}} = e^{-2\pi i\frac{j\left(\langle\mathbf{b},\mathbf{w}\rangle+\frac{v_1'}{D}\right)}{\frac{M}{2D}}}$. Therefore, running over the summation of $j\in\mathbb{Z}$, the amplitude on $|\mathbf{w}\rangle$ will only be non-zero when $\langle\mathbf{b},\mathbf{w}\rangle+\frac{v_1'}{D}\equiv 0 \pmod{\frac{M}{2D}}$.

Then, to see the impact of the summation over $\mathbf{k} \in 0 \mid \mathbb{Z}^{n-1}$ on the amplitude of $\mathbf{w}$, we observe that

$$\sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}} e^{2\pi i\left(\frac{\|\mathbf{k}\|^2}{4}-\frac{\langle \mathbf{k},\mathbf{w}\rangle}{2D}\right)} = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}} e^{\pi i\frac{\|\mathbf{k}\|^2}{2}} e^{-2\pi i\frac{\langle \mathbf{k},\mathbf{w}\rangle}{2D}}$$
$$= \sum_{\mathbf{l}\in\mathbb{Z}^{n-1}} e^{-2\pi i\|\mathbf{l}+\frac{\mathbf{w}_{[2\ldots n]}}{2D}\|^2} = \sum_{\mathbf{l}\in\mathbb{Z}^{n-1}} e^{-2\pi i\left\langle \mathbf{l},\frac{\mathbf{w}_{[2\ldots n]}}{D}\right\rangle} e^{-2\pi i\|\frac{\mathbf{w}_{[2\ldots n]}}{2D}\|^2}.$$

Therefore the amplitude of $|\varphi_{7.d}\rangle$ can be written as

$$|\varphi_{7.d}\rangle = \sum_{\mathbf{w}\in\mathbb{Z}_M^n}\sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{j\left(\langle \mathbf{b},\mathbf{w}\rangle+\frac{v_1'}{D}\right)}{\frac{M}{2D}}} e^{-2\pi i\frac{\left\langle \frac{\mathbf{v}'}{D},\mathbf{w}\right\rangle}{M}} \sum_{\mathbf{l}\in\mathbb{Z}^{n-1}} e^{-2\pi i\left\langle \mathbf{l},\frac{\mathbf{w}_{[2\ldots n]}}{D}\right\rangle} e^{-2\pi i\|\frac{\mathbf{w}_{[2\ldots n]}}{2D}\|^2} |\mathbf{w}\rangle .$$

Due to the summation over $\mathbf{l} \in \mathbb{Z}^{n-1}$, the amplitude on $|\mathbf{w}\rangle$ will only be non-zero when $\frac{\mathbf{w}_{[2\ldots n]}}{D} \in \mathbb{Z}^{n-1}$. Finally, we recall from Eqn. (12) that $\mathbf{b} \in (-1) \mid 2p_1\mathbb{Z}^{n-1}$, so we always have $\left\langle \mathbf{b}_{[2\ldots n]}, \mathbf{w}_{[2\ldots n]}\right\rangle \in 2Dp_1$. Also recall from **C.3** that Dp_1 is a factor of $\frac{M}{2D}$, therefore $w_1 \equiv \frac{v_1'}{D} \pmod{Dp_1}$. □

Therefore, in the fifth operation, we compute $w_1 \bmod Dp_1$ in a new register, then measure the new register $|w_1 \bmod Dp_1\rangle$ and denote the result as $w_1' = \frac{v_1'}{D} \bmod Dp_1$. This measurement does not collapse the state $|\varphi_{7.d}\rangle$, so the residual state is $|\varphi_{7.e}\rangle = |\varphi_{7.d}\rangle$.

Next we reverse the previous four operations and get back to

$$|\varphi_8\rangle = |\varphi_7\rangle = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1},j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} e^{2\pi i\frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{x}+\mathbf{v}'+\frac{M}{2}\mathbf{k} \bmod M\right\rangle .$$

In other words, in Step 8, we learn $v_1' \bmod D^2p_1$ without affecting the state $|\varphi_7\rangle$ at all. □

Readers may wonder why are the first two operations necessary, or, can we remove the quadratic amplitude on j directly from $|\varphi_7\rangle$? We may try to use the phase kickback trick on the first coordinate of $|\varphi_7\rangle$, $-2D^2j + v_1' \bmod M$, to multiply $e^{2\pi i\frac{(-2D^2j+v_1' \bmod M)^2}{2D^2M}}$ on the amplitude of $|\varphi_7\rangle$, but the modulo M sign does not go away in the exponent. If we apply $\mathsf{QFT}_{\mathbb{Z}_M^n}$ after it, we get a state where the support does not satisfy a modular linear function, unlike $|\varphi_{7.d}\rangle$ in our algorithm. See Figure 3 for a comparison of $|\varphi_{7.d}\rangle$ in our real algorithm, and what we get if apply the phase kick-back trick directly on $|\varphi_7\rangle$, and then apply $\mathsf{QFT}_{\mathbb{Z}_M^n}$.

3.5.9 Step 9: Extract a linear equation over the secret from $v_1' \bmod D^2p_1$ and $|\varphi_8\rangle$

In Step 9, our goal is to convert $|\varphi_8\rangle$ into a classical linear equation over the secret, which finally gives a proof of the main lemma (Lemma 3.8). Step 9 uses the information of $v_1' \bmod D^2p_1$ obtained in Step 8, and the $\kappa - 1$ coordinates of known items inserted in the LWE secret.

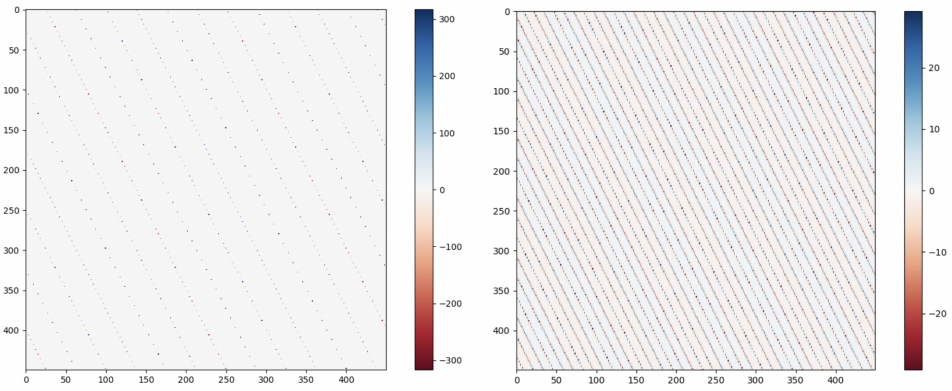

Figure 3: Comparison of the real part of the amplitude in $|\varphi_{7.d}\rangle$ (left) and a state obtained after directly applying phase kickback on $|\varphi_7\rangle$, and then applying QFT (right). Parameters are set in the same way as the ones in Figure 2, except that we set $D = 3$ here. The left figure is similar to Figure 2 - (i). For the figure on the right, the amplitude is non-zero almost everywhere (the light blue and light red ones are non-zero).

Proof of Lemma 3.8. Recall from **C.3** that $M = 2D^2(c+1)\|\mathbf{b}\|^2 = 2D^2 p_1 p_2 ... p_\kappa$, where D, p_1, ..., p_k are odd and pairwise coprime. Start from $|\varphi_8\rangle = \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i \frac{(2Dj)^2}{2M}} e^{2\pi i \frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{x} + \mathbf{v}' + \frac{M}{2}\mathbf{k} \bmod M\right\rangle$, we first compute every coordinate into its Chinese remainder theorem (CRT) representation modulo 2 and modulo $\frac{M}{2} = D^2 p_1 p_2 ... p_\kappa$, and denote the state as $|\varphi_{8.a}\rangle$ (note that computing the CRT representation is an efficient, reversible operation so it can be efficiently done quantumly):

$$
\begin{aligned}
|\varphi_{8.a}\rangle &:= \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i \frac{(2Dj)^2}{2M}} e^{2\pi i \frac{\|\mathbf{k}\|^2}{4}} \left|2Dj\mathbf{x} + \mathbf{v}' + \frac{M}{2}\mathbf{k} \bmod D^2 p_1 p_2 ... p_\kappa\right\rangle \left|2Dj\mathbf{x} + \mathbf{v}' + \frac{M}{2}\mathbf{k} \bmod 2\right\rangle \\
&= \sum_{\mathbf{k}\in 0|\mathbb{Z}^{n-1}, j\in\mathbb{Z}} e^{-2\pi i \frac{(2Dj)^2}{2M}} e^{2\pi i \frac{\|\mathbf{k}\|^2}{4}} \left|2D^2 j\mathbf{b} + \mathbf{v}' \bmod D^2 p_1 p_2 ... p_\kappa\right\rangle \left|\mathbf{v}' + \frac{M}{2}\mathbf{k} \bmod 2\right\rangle .
\end{aligned}
$$

We then measure the "modulo 2" part and throw it away, which completely collapses $\mathbf{k}$ but not affects j, so that the residual state $|\varphi_{8.b}\rangle$ is independent of $\mathbf{k}$:

$$
|\varphi_{8.b}\rangle := \sum_{j\in\mathbb{Z}} e^{-2\pi i \frac{(2Dj)^2}{2M}} \left|2D^2 j\mathbf{b} + \mathbf{v}' \bmod D^2 p_1 p_2 ... p_\kappa\right\rangle .
$$

Next we turn the first κ coordinates of $|\varphi_{8.b}\rangle$ into their CRT representations modulo D^2p_1, p_2, ..., p_κ:

$$\begin{aligned}
|\varphi_{8.c}\rangle := \sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} &\left|2D^2jb_1 + v'_1 \bmod D^2p_1\right\rangle \left|2D^2jb_1 + v'_1 \bmod p_2\right\rangle ... \left|2D^2jb_1 + v'_1 \bmod p_\kappa\right\rangle \\
&\left|2D^2jb_2 + v'_2 \bmod D^2p_1\right\rangle \left|2D^2jb_2 + v'_2 \bmod p_2\right\rangle ... \left|2D^2jb_2 + v'_2 \bmod p_\kappa\right\rangle \\
&... \left|2D^2jb_\kappa + v'_\kappa \bmod D^2p_1\right\rangle \left|2D^2jb_\kappa + v'_\kappa \bmod p_2\right\rangle ... \left|2D^2jb_\kappa + v'_\kappa \bmod p_\kappa\right\rangle \\
&\left|2D^2j\mathbf{b}_{[\kappa+1...n]} + \mathbf{v}'_{[\kappa+1...n]} \bmod D^2p_1p_2...p_\kappa\right\rangle \\
= \sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} &\left|2D^2jb_1 + v'_1 \bmod D^2p_1\right\rangle \left|2D^2jb_1 + v'_1 \bmod p_2\right\rangle ... \left|2D^2jb_1 + v'_1 \bmod p_\kappa\right\rangle \\
&\left|2D^2jb_2 + v'_2 \bmod D^2p_1\right\rangle \left|v'_2 \bmod p_2\right\rangle ... \left|2D^2jb_2 + v'_2 \bmod p_\kappa\right\rangle \\
&... \left|2D^2jb_\kappa + v'_\kappa \bmod D^2p_1\right\rangle \left|2D^2jb_\kappa + v'_\kappa \bmod p_2\right\rangle ... \left|v'_\kappa \bmod p_\kappa\right\rangle \\
&\left|2D^2j\mathbf{b}_{[\kappa+1...n]} + \mathbf{v}'_{[\kappa+1...n]} \bmod D^2p_1p_2...p_\kappa\right\rangle,
\end{aligned}$$

where the second equality holds since $\mathbf{b}_{[1...\kappa]} = (-1, 2p_1p_2, 2p_1p_3, ..., 2p_1p_\kappa)$ (see Eqn. (12)), so that the $|v'_2 \bmod p_2\rangle$, $|v'_3 \bmod p_3\rangle$, ..., $|v'_\kappa \bmod p_\kappa\rangle$ registers are independent of j. (In fact, $\left|2D^2jb_2 + v'_2 \bmod D^2p_1\right\rangle$, ..., $\left|2D^2jb_\kappa + v'_\kappa \bmod D^2p_1\right\rangle$ are also independent of j, but we will not utilize this fact.)

We then measure $|v'_2 \bmod p_2\rangle$, $|v'_3 \bmod p_3\rangle$, ..., $|v'_\kappa \bmod p_\kappa\rangle$ and learn $v'_2 \bmod p_2$, $v'_3 \bmod p_3$, ..., $v'_\kappa \bmod p_\kappa$ without collapsing the states (i.e., we can add them in new registers and measure the new registers, which doesn't collapse $|v'_2 \bmod p_2\rangle$, ..., $|v'_\kappa \bmod p_\kappa\rangle$ and others).

Next, for all $\eta \in \{2, 3, ..., \kappa\}$, we swap $\left|v'_\eta \bmod p_\eta\right\rangle$ in the η^{th} coordinate with $\left|2D^2jb_1 + v'_1 \bmod p_\eta\right\rangle$ in the 1^{st} coordinate (swapping is an efficient, reversible operation so it can be efficiently done quantumly), and get the following state (we use underline to highlight the swapped registers)

$$\begin{aligned}
|\varphi_{8.d}\rangle := \sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} &\left|2D^2jb_1 + v'_1 \bmod D^2p_1\right\rangle \underline{\left|v'_2 \bmod p_2\right\rangle} ... \underline{\underline{\left|v'_\kappa \bmod p_\kappa\right\rangle}} \\
&\left|2D^2jb_2 + v'_2 \bmod D^2p_1\right\rangle \underline{\left|2D^2jb_1 + v'_1 \bmod p_2\right\rangle} \left|2D^2jb_2 + v'_2 \bmod p_3\right\rangle ... \left|2D^2jb_2 + v'_2 \bmod p_\kappa\right\rangle \\
&... \left|2D^2jb_\kappa + v'_\kappa \bmod D^2p_1\right\rangle \left|2D^2jb_\kappa + v'_\kappa \bmod p_2\right\rangle ... \left|2D^2jb_\kappa + v'_\kappa \bmod p_{\kappa-1}\right\rangle \underline{\underline{\left|2D^2jb_1 + v'_1 \bmod p_\kappa\right\rangle}} \\
&\left|2D^2j\mathbf{b}_{[\kappa+1...n]} + \mathbf{v}'_{[\kappa+1...n]} \bmod D^2p_1p_2...p_\kappa\right\rangle.
\end{aligned}$$

Let $\mathsf{CRT}((a_1)_{D^2p_1}, (a_2)_{p_2}, ..., (a_\kappa)_{p_\kappa})$ denote the mapping from the CRT representation of a number in $\mathbb{Z}_{D^2p_1} \times \mathbb{Z}_{p_2} \times ... \times \mathbb{Z}_{p_\kappa}$ back to its standard representation in $\mathbb{Z}_{D^2p_1...p_\kappa}$ (the mapping is efficiently computable). Then, let $\mathbf{b}^* \in \mathbb{Z}^n_{p_1...p_\kappa}$, $\mathbf{v}^* \in \mathbb{Z}^n_{D^2p_1...p_\kappa}$ be defined as

$$\begin{aligned}
2D^2b^*_1 &:= \mathsf{CRT}((2D^2b_1)_{D^2p_1}, (0)_{p_2}, ..., (0)_{p_\kappa}), && \% \text{ known} \\
v^*_1 &:= \mathsf{CRT}((v'_1)_{D^2p_1}, (v'_2)_{p_2}, ..., (v'_\kappa)_{p_\kappa}), && \% \text{ known} \\
2D^2b^*_\eta &:= \mathsf{CRT}((2D^2b_\eta)_{D^2p_1}, (2D^2b_\eta)_{p_2}, ..., (2D^2b_1)_{p_\eta}, ..., (2D^2b_\eta)_{p_\kappa}), && \% \text{ known} \\
v^*_\eta &:= \mathsf{CRT}((v'_\eta)_{D^2p_1}, (v'_\eta)_{p_2}, ..., (v'_1)_{p_\eta}, ..., (v'_\eta)_{p_\kappa}), \quad \forall \eta \in \{2, 3, ..., \kappa\}, && \% \text{ unknown} \\
\mathbf{b}^*_{[\kappa+1...n]} &:= \mathbf{b}_{[\kappa+1...n]}, \quad \mathbf{v}^*_{[\kappa+1...n]} := \mathbf{v}'_{[\kappa+1...n]}. && \% \text{ both unknown}
\end{aligned} \tag{36}$$

Then, in the next operation, we switch the first κ coordinates from the CRT representation back to the standard representation in $\mathbb{Z}_{D^2 p_1 \dots p_k}$. We get

$$|\varphi_{8.e}\rangle := \sum_{j\in\mathbb{Z}} e^{-2\pi i \frac{(2Dj)^2}{2M}} \left|2D^2 j\mathbf{b}^* + \mathbf{v}^* \bmod D^2 p_1 p_2 \dots p_\kappa\right\rangle.$$

Now $v_1^* = \mathsf{CRT}((v_1')_{D^2 p_1}, (v_2')_{p_2}, ..., (v_\kappa')_{p_\kappa})$ is efficiently computable (recall that we learned $v_1' \bmod D^2 p_1$ in Step 8, and learned $v_2' \bmod p_2$, ..., $v_\kappa' \bmod p_\kappa$ after obtaining $|\varphi_{8.c}\rangle$). So we can subtract v_1^* modulo $D^2 p_1 \dots p_\kappa$ in the first coordinate and get

$$|\varphi_{8.f}\rangle := \sum_{j\in\mathbb{Z}} e^{-2\pi i \frac{(2Dj)^2}{2M}} \left|2D^2 j\mathbf{b}^* + 0 \mid \mathbf{v}^*_{[2\dots n]} \bmod D^2 p_1 p_2 \dots p_\kappa\right\rangle. \tag{37}$$

We can derive from Eqn. (36) and Cond. **C.3** that $b_1^* = p_2 p_3 \dots p_\kappa \cdot (-(p_2 p_3 \dots p_\kappa)^{-1} \bmod p_1) = p_2 p_3 \dots p_\kappa$. We hope to change $|\varphi_{8.f}\rangle$ so that the j in the first coordinate of $\left|2D^2 j\mathbf{b}^* + 0 \mid \mathbf{v}^*_{[2\dots n]} \bmod D^2 p_1 p_2 \dots p_\kappa\right\rangle$ runs through all $j \in \mathbb{Z}_{p_1 p_2 \dots p_\kappa}$, but currently the j in the first coordinate only runs through $\mathbb{Z}_{p_1}$. So we apply the domain extension trick (Lemma 2.17) on the first coordinate of $|\varphi_{8.f}\rangle$ to extend the domain of the first coordinate from $D^2 p_1 p_2 \dots p_\kappa$ to $D^2 p_1 p_2 \dots p_\kappa \cdot p_2 \dots p_\kappa$, and get

$$|\varphi_{8.g}\rangle := \sum_{j\in\mathbb{Z}} e^{-2\pi i \frac{(2Dj)^2}{2M}} \left|2D^2 j\mathbf{b}_1^* \bmod D^2 p_1 p_2 \dots p_\kappa \cdot p_2 \dots p_\kappa\right\rangle \left|2D^2 j\mathbf{b}^*_{[2\dots n]} + \mathbf{v}^*_{[2\dots n]} \bmod D^2 p_1 p_2 \dots p_\kappa\right\rangle.$$

To see why applying domain extension gives the desired expression $|\varphi_{8.g}\rangle$, we double check the $\frac{M}{2}$-periodicity of the amplitude of $|\varphi_{8.f}\rangle$ in Eqn. (37). There are two methods to check it. The first method is to make sure no operation after Step 7 breaks the $\frac{M}{2}$-periodicity: the operations from Step 7 up to Step 8 preserve M-periodicity, and after measuring out the modulo 2 part in the beginning of Step 9, the rest of operations (such as computing the CRT representation, swapping the same CRT slot between coordinates) preserve the $\frac{M}{2}$-periodicity. The second method is to verify $\frac{M}{2}$-periodicity directly: although the period of j in the first coordinate is p_1, the period of j in the last $n-1$ coordinates is $p_2 \dots p_\kappa$ since $\mathbf{b}^*_{[2\dots n]} \in 2p_1\mathbb{Z}$, and 2 is invertible mod $\frac{M}{2}$. So for any $\mathbf{z} = 2D^2 j\mathbf{b}^* + 0 \mid \mathbf{v}^*_{[2\dots n]} \bmod \frac{M}{2}$, if we want to write $\mathbf{z}$ as

$$\mathbf{z} = 2D^2(j+j')\mathbf{b}^* + 0 \mid \mathbf{v}^*_{[2\dots n]} \bmod \frac{M}{2} \text{ for some } j' \in \mathbb{Z},$$

then it must be the case that $j' \in p_1 p_2 \dots p_\kappa \mathbb{Z} = \frac{M}{2D^2}\mathbb{Z}$; and for all $j \in \mathbb{Z}$, we have

$$e^{-2\pi i \frac{(2D)^2\left(j+\frac{M}{2D^2}\right)^2}{2M}} = e^{-2\pi i \frac{(2D)^2\left(j^2 + j\frac{M}{D^2} + \left(\frac{M}{2D^2}\right)^2\right)}{2M}} = e^{-2\pi i \frac{(2D)^2 j^2 + 4Mj + \frac{M^2}{D^2}}{2M}} = {}_{\frac{M}{2D^2}\in\mathbb{Z}}\ e^{-2\pi i \frac{(2D)^2 j^2}{2M}}.$$

This verifies the $\frac{M}{2}$-periodicity of the amplitude of $|\varphi_{8.f}\rangle$ in Eqn. (37).

Let us continue working on $|\varphi_{8.g}\rangle$. Since $b_1^* = p_2 p_3 \dots p_\kappa$, we divide the first coordinate by $p_2 \dots p_\kappa$ (i.e., just measure out the first coordinate modulo $p_2 \dots p_\kappa$, which will return 0, and then we interpret the

remaining first coordinate as being divided by $p_2...p_\kappa$). This gives

$$\begin{aligned}|\varphi_{8.h}\rangle :=& \sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} \left|2D^2 j \bmod D^2 p_1p_2...p_\kappa\right\rangle \left|2D^2 j\mathbf{b}^*_{[2...n]} + \mathbf{v}^*_{[2...n]} \bmod D^2p_1p_2...p_\kappa\right\rangle \\ =& \sum_{j\in\mathbb{Z}_{p_1p_2\cdots p_\kappa}} e^{-2\pi i\frac{(2Dj)^2}{2M}} \left|2D^2 j \bmod D^2 p_1p_2...p_\kappa\right\rangle \left|2D^2 j\mathbf{b}^*_{[2...n]} + \mathbf{v}^*_{[2...n]} \bmod D^2p_1p_2...p_\kappa\right\rangle,\end{aligned}$$

where in the second line we change from $j \in \mathbb{Z}$ to $j \in \mathbb{Z}_{p_1p_2...p_\kappa}$ because now it is more convenient to work with j over $\mathbb{Z}_{p_1p_2...p_\kappa}$.

Next we apply the phase kickback trick on the first coordinate of $|\varphi_{8.h}\rangle$ to multiply the phase term $e^{2\pi i\frac{(2Dj)^2}{2M}}$ on the amplitude. We can do so since $\frac{(2Dj)^2}{2M} = \frac{j^2}{p_1p_2...p_\kappa}$ is efficiently computable from $D^2 \cdot 2j \bmod D^2p_1p_2...p_\kappa$. This gives

$$|\varphi_{8.i}\rangle := \sum_{j\in\mathbb{Z}_{p_1p_2\cdots p_\kappa}} \left|2D^2 \cdot j \bmod D^2 p_1p_2...p_\kappa\right\rangle \left|2D^2 j\mathbf{b}^*_{[2...n]} + \mathbf{v}^*_{[2...n]} \bmod D^2p_1p_2...p_\kappa\right\rangle.$$

Finally, we apply $\mathsf{QFT}_{\mathbb{Z}^n_{D^2p_1p_2\cdots p_\kappa}}$ on $|\varphi_{8.i}\rangle$ and get

$$|\varphi_9\rangle := \sum_{\mathbf{u}\in\mathbb{Z}^n_{D^2p_1p_2\cdots p_\kappa}} \sum_{j\in\mathbb{Z}_{p_1p_2\cdots p_\kappa}} e^{-2\pi i\cdot 2j\cdot\frac{u_1+\left\langle\mathbf{b}^*_{[2...n]},\mathbf{u}_{[2...n]}\right\rangle}{p_1p_2\cdots p_\kappa}} e^{-2\pi i\frac{\left\langle\mathbf{v}^*_{[2...n]},\mathbf{u}_{[2...n]}\right\rangle}{D^2p_1p_2\cdots p_\kappa}} |\mathbf{u}\rangle.$$

We measure $|\mathbf{u}\rangle$ to get a random $\mathbf{u} \in \mathbb{Z}^n_{D^2p_1p_2...p_\kappa}$ satisfying

$$u_1 + \left\langle\mathbf{b}^*_{[2...n]}, \mathbf{u}_{[2...n]}\right\rangle \equiv 0 \pmod{p_1p_2...p_\kappa}. \tag{38}$$

Recall the expression of $\mathbf{b}^*_{[2...n]}$ from Eqn. (36), the $\mathbf{b}^*_{[2...\kappa]}$ part is efficiently computable, and $\mathbf{b}^*_{[\kappa+1...n]} = \mathbf{b}_{[\kappa+1...n]} =_{Eqn.\ (12)} [2p_1\mathbf{s}^T_{[\kappa...\ell]}, 2p_1\mathbf{e}^T]^T$, containing all the unknown secret and error terms we want to learn. So we return $\mathbf{u} \in \mathbb{Z}^n_{\frac{M}{2}}$ as the coefficient of a linear equation over all the unknown variables we care about.

This completes the proof of Lemma 3.8. □

Readers may wonder: given the power of the swapping trick used between $|\varphi_{8.c}\rangle$ and $|\varphi_{8.d}\rangle$, why can't we simply plant a trivial mod p_1 slot as well and swap it to the first coordinate, instead of spending so much effort in learning $v'_1 \bmod D^2p_1$ in Step 8. In fact, why can't we swap $\left|2D^2jb_1 + v'_1 \bmod D^2p_1\right\rangle$ and $\left|2D^2jb_2 + v'_2 \bmod D^2p_1\right\rangle$ as well, since we know $b_2 = 2p_1p_2$, so $v'_2 \bmod D^2p_1$ can be learned for free. The reason is: if we use the swap trick to prepare for the mod p_1 slot as well, then after swapping, the first coordinate will be completely independent of j, and then the first coordinate is useless. Therefore, it is crucial that we learn one of the CRT components of v'_1 in a non-trivial way.

Readers may also wonder: given the power of the domain extension trick applied between $|\varphi_{8.f}\rangle$ and $|\varphi_{8.g}\rangle$, can we use the domain extension trick to solve the dihedral coset problem (DCP) right away?

To answer this question, recall a typical instance of (the vector version of) DCP, where we are given quantum states like

$$\sum_{j\in\{0,1\}} |j\rangle\,|j\mathbf{x}-\mathbf{y} \bmod P\rangle = \sum_{j\in\{0,1\}} |j\rangle\,|(j \bmod 2)\mathbf{x}-\mathbf{y} \bmod P\rangle\,. \tag{39}$$

Suppose $P \in 2\mathbb{Z}$. How about we apply the domain extension trick to extend the first coordinate to work over all $\mathbb{Z}_P$? We can do this operation but we will get a state like $\sum_{j\in\mathbb{Z}_P} |j\rangle\,|(j \bmod 2)\mathbf{x}-\mathbf{y} \bmod P\rangle$, which, for a general $\mathbf{x} \in \mathbb{Z}_P^n$, is not equal to $\sum_{j\in\mathbb{Z}_P} |j\rangle\,|j\mathbf{x}-\mathbf{y} \bmod P\rangle$. Then applying $\mathsf{QFT}_{\mathbb{Z}_P^{n+1}}$ on $\sum_{j\in\mathbb{Z}_P} |j\rangle\,|(j \bmod 2)\mathbf{x}-\mathbf{y} \bmod P\rangle$ does not seem to give a useful state for extracting $\mathbf{x}$.

In our application of the domain extension trick after $|\varphi_{8.f}\rangle$ in Eqn. (37), we note that

$$|\varphi_{8.f}\rangle \neq \sum_{j\in\mathbb{Z}} e^{-2\pi i\frac{(2Dj)^2}{2M}} \left|2D^2(j \bmod p_1)\mathbf{b}^* + 0 \mid \mathbf{v}^*_{[2\ldots n]} \bmod D^2 p_1 p_2 \ldots p_\kappa\right\rangle,$$

therefore we will not meet the problem occurred in Eqn. (39). In other words, it is crucial in $|\varphi_{8.f}\rangle$ that the j in the last $n-1$ coordinates goes through all $\mathbb{Z}_{p_2\ldots p_\kappa}$. It is also crucial to check the $\frac{M}{2}$-periodicity of the amplitude of $|\varphi_{8.f}\rangle$ before applying domain extension, as we have done in the paragraph after presenting $|\varphi_{8.g}\rangle$.

This concludes the description of all the nine quantum steps.

3.6 Detailed proofs

In this section we provide the detailed proofs missed in Section 3.5. All proofs except for the proof of Lemma 3.7 are about Fourier transforms and Gaussian tail bounds over discrete supports. Let us remark that all Gaussian tail bounds here are essentially proven using one of the following two methods: a sophisticated method from [Reg23, Claim A.5] (adapted to ℓ_∞ norm in our paper), which gives nearly optimal bounds; and a more straightforward method by using ℓ_2, ℓ_1 norm inequalities (like in Lemma 3.10), which gives fairly loose bounds, but is much simpler to calculate. Only the proof of Lemma 3.20 uses the sophisticated method, because getting an optimal bound there matters to the quality of our algorithm. The other bounds are proved using the straightforward method for simplicity because the loose bounds suffice for our purpose.

3.6.1 Proof of Lemma 3.7

Proof. Recall from §3.2 that $\mathbf{U} \leftarrow U(\mathbb{Z}_q^{n\times m})$, $\mathbf{t} = \mathbf{U}^T\mathbf{s} + \mathbf{e} \bmod q$ where $\mathbf{s}_{[\kappa\ldots\ell]} \leftarrow D_{\mathbb{Z},\beta}^{\ell-(\kappa-1)}, \mathbf{e} \leftarrow D_{\mathbb{Z},\beta}^m$. Recall from Eqn. (12) that $\mathbf{A} = [2p_1\mathbf{t} \mid \mathbf{U}^T \mid \mathbf{I}_m] \in \mathbb{Z}_q^{m\times n}$, $\mathbf{b} = [-1, 2p_1\mathbf{s}^T, 2p_1\mathbf{e}^T]^T = [-1, 2p_1p_2, \ldots, 2p_1p_\kappa, 2p_1\mathbf{s}^T_{[\kappa\ldots\ell]}, 2p_1\mathbf{e}^T]^T$. Then $\mathbf{b} \in L_q^\perp(\mathbf{A})$ and $\|\mathbf{b}\| \le 3p_1\beta\sqrt{n} < \frac{q}{(\log n)^2}$ due to Lemma 3.6.

It remains to prove the following claim:

Claim 3.15. *With probability* $1-\mathrm{negl}(n)$ *over the randomness of sampling* $\mathbf{U}$, $\mathbf{t}$, *for any non-zero vector* $\mathbf{z} = [-d, \mathbf{z}_1^T, \mathbf{z}_2^T]^T \in L_q^\perp(\mathbf{A})$, *where* $\mathbf{z}_1 \in \mathbb{Z}^\ell$, $\mathbf{z}_2 \in \mathbb{Z}^m$, $d \in \mathbb{Z} \cap (-q/(\log n)^2, q/(\log n)^2)$, *we have either* $\mathbf{z} = \mathbf{b}d$ *(in which case* $\mathbf{z}$ *is linearly dependent on* $\mathbf{b}$*), or* $\|\mathbf{z}\|_\infty \ge q/(\log n)^2$.

Note that we don't need to consider those d s.t. $|d| \geq q/(\log n)^2$ since that immediately leads to $\|\mathbf{z}\|_\infty \geq q/(\log n)^2$.

Proof of Claim 3.15. Given that $\mathbf{z} = [-d, \mathbf{z}_1^T, \mathbf{z}_2^T]^T \in L_q^\perp(\mathbf{A})$, we have

$$\mathbf{U}^T\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{t}d \equiv \mathbf{U}^T(\mathbf{z}_1 - 2p_1 d\mathbf{s}) - 2p_1 d\mathbf{e} + \mathbf{z}_2 \equiv \mathbf{0} \pmod q. \tag{40}$$

We observe that Eqn. (40) is satisfiable either when $\mathbf{z}_1 - 2p_1 d\mathbf{s} \equiv \mathbf{0} \pmod q$, or $\mathbf{z}_1 - 2p_1 d\mathbf{s} \not\equiv \mathbf{0} \pmod q$.

If $\mathbf{z}_1 - 2p_1 d\mathbf{s} \not\equiv \mathbf{0} \pmod q$, then we can apply Lemma 2.10 with $\mathcal{V} := \{2p_1 d\mathbf{e}\}_{d \in \mathbb{Z} \cap (-q/(\log^2 n), q/(\log^2 n))}$ (the matrix $\mathbf{A}$ in Lemma 2.10 is the matrix $\mathbf{U}$ here). This implies that with probability $1 - 2^{-\Omega(n)}$, $\|\mathbf{z}_2\|_\infty \geq q/4$, so $\lambda_2^\infty\left(L_q^\perp(\mathbf{A})\right) \geq q/4 \geq q/(\log n)^2$.

If $\mathbf{z}_1 - 2p_1 d\mathbf{s} \equiv \mathbf{0} \pmod q$, then $\mathbf{z}_2 - 2p_1 d\mathbf{e} \equiv \mathbf{0} \pmod q$ as well. In this case,

1. either $\mathbf{z} = \mathbf{b}d$ holds over $\mathbb{Z}^n$, without mod q – then $\mathbf{z}$ is linearly dependent on $\mathbf{b}$, so the length of $\mathbf{z}$ does not influence the value of $\lambda_2^\infty\left(L_q^\perp(\mathbf{A})\right)$;
2. or $\mathbf{z} = \mathbf{b}d + q\mathbf{k}$ for some non-zero $\mathbf{k} \in \mathbb{Z}^n$ (i.e., $\mathbf{z} \equiv \mathbf{b}d \pmod q$ must use mod q) – if $\|\mathbf{z}\|_\infty < q/(\log^2 n)$ in this case then $\lambda_2^\infty\left(L_q^\perp(\mathbf{A})\right) < q/(\log^2 n)$, so we need to handle this case carefully.

The rest of the proof is devoted to proving the following claim:

Claim 3.16. *For any $n \in \mathbb{N}^+$, any integer $q \geq (\log n)^2$. For any real number $\beta > 0$,*

$$\Pr_{\mathbf{b}}\left[\exists \mathbf{z} \in \mathbb{Z}^n \cap \frac{q}{(\log n)^2}\mathcal{B}_\infty^n \text{ s.t. } \mathbf{z} = \mathbf{b}d + q\mathbf{k} \text{ for some non-zero } \mathbf{k} \in \mathbb{Z}^n, d \in \mathbb{Z}, |d| < \frac{q}{(\log n)^2}\right] < \mathrm{negl}(n),$$

where the randomness over $\mathbf{b}$ comes from the sampling of $\mathbf{s}_{[\kappa \ldots \ell]} \leftarrow D_{\mathbb{Z},\beta}^{\ell-(\kappa-1)}, \mathbf{e} \leftarrow D_{\mathbb{Z},\beta}^m$.

Proof. First we observe that Claim 3.16 is true when $\beta \leq \log n$, since in this case $2p_1 d\beta \leq 2p_1 \frac{q}{\log n}$, so $d\mathbf{b} \leq q/2$ with probability $1 - \mathrm{negl}(n)$ due to Lemma 2.6.

Second, when $\beta > \log n$, we only need to consider the case where $d > \frac{q}{\beta \log n}$ (therefore $2p_1 d\beta > 2p_1 \frac{q}{\log n}$), since if $d \leq \frac{q}{\beta \log n}$, then $\|\mathbf{b}d\|_\infty > q/2$ with probability negligible in n due to Lemma 2.6 (this means $\mathbf{z} = \mathbf{b}d + q\mathbf{k}$ for some non-zero $\mathbf{k} \in \mathbb{Z}^n$ happens with negligible probability in n).

So it remains to deal with the case where $\frac{q}{\beta \log n} < d < \frac{q}{(\log n)^2}$.

Claim 3.17. *For any $n \in \mathbb{N}^+$, any integer $q \geq (\log n)^2$. For any real number $\beta > \log n$, for any integer $d \in \left(\frac{q}{\beta \log n}, \frac{q}{(\log n)^2}\right)$,*

$$\Pr_{y \leftarrow D_{\mathbb{Z},\beta}}\left[2p_1 d \cdot y \in q\mathbb{Z} + \left(-\frac{q}{(\log n)^2}, \frac{q}{(\log n)^2}\right)\right] < \frac{1}{4}.$$

Proof. If y was sampled from the continuous Gaussian distribution D_β, then the proof can be done by just taking integrals. Here since y is sampled from the discrete Gaussian distribution $D_{\mathbb{Z},\beta}$, we need some properties of smoothing parameters. Let us introduce them first.

A special case of [Pei10, Theorem 3.1] shows that when s is large enough, $D_{\mathbb{Z},s}$ is statistically close to rounding a continuous Gaussian.

Lemma 3.18. *For any $\epsilon < 1/8$, and $s > \eta_\epsilon(\mathbb{Z})$. Then $\lfloor D_s \rceil$ is within statistical distance 8ϵ from $D_{\mathbb{Z},s}$.*

A special case of [MR07, Lemma 4.1] shows that:

Lemma 3.19. *For any $\epsilon, t \in \mathbb{R}^+$, for any $s \geq \eta_\epsilon(t\mathbb{Z})$, the statistical distance between $D_s \bmod t$ and $U([0,t))$ is within $\epsilon/2$.*

Our proof therefore goes through two intermediate steps. First, we consider $2p_1 dy \leftarrow \lfloor D_{2p_1 d\beta} \rceil_{2p_1 d}$ instead of $2p_1 dy \leftarrow 2p_1 d \cdot D_{\mathbb{Z},\beta}$ since they are statistically close due to Lemma 3.18. Second, we choose $t \in \mathbb{Q}$ such that $t \in 2p_1 \left(\frac{20q}{(\log n)^2}, \frac{40q}{(\log n)^2}\right)$ and $\frac{q}{t} \in \mathbb{N}^+$ (we choose $t \in \mathbb{Q}$ instead of $t \in \mathbb{Z}$ since there always exists a t in $2p_1 \left(\frac{20q}{(\log n)^2}, \frac{40q}{(\log n)^2}\right) \cap \mathbb{Q}$, but $2p_1 \left(\frac{20q}{(\log n)^2}, \frac{40q}{(\log n)^2}\right) \cap \mathbb{Z}$ can be empty, e.g., when q is a prime), and we consider $2p_1 dy \leftarrow U([0,t))$ instead of $\lfloor D_{2p_1 d\beta} \rceil_{2p_1 d} \bmod t$ since they are statistically close due to Lemma 3.19. Over $U([0,t))$ it is then easy to prove the result we want.

Formally, for any integer $d < \frac{q}{(\log n)^2}$, for any $t \in \mathbb{Q}$ such that $t \in 2p_1 \left(\frac{20q}{(\log n)^2}, \frac{40q}{(\log n)^2}\right)$ and $\frac{q}{t} \in \mathbb{N}^+$,

$$\Pr_{z \leftarrow U([0,t))} \left[\lfloor z \rceil_{2p_1 d} \in t\mathbb{Z} + \left(-\frac{q}{(\log n)^2}, \frac{q}{(\log n)^2} \right) \right] \leq \frac{1}{5}.$$

Then, since $2p_1 d\beta > 2p_1 \frac{q}{\log n} \in \frac{q}{(\log n)^2} \cdot \omega(\sqrt{\log n})$, we have

$$\begin{aligned}
& \Pr_{z \leftarrow D_{2p_1 d\beta}} \left[\lfloor z \rceil_{2p_1 d} \in q\mathbb{Z} + \left(-\frac{q}{(\log n)^2}, \frac{q}{(\log n)^2} \right) \right] \\
\leq_{(a)} \; & \Pr_{z \leftarrow D_{2p_1 d\beta}} \left[\lfloor z \rceil_{2p_1 d} \in t\mathbb{Z} + \left(-\frac{q}{(\log n)^2}, \frac{q}{(\log n)^2} \right) \right] \qquad (41) \\
\leq_{(b)} \; & \Pr_{z \leftarrow U([0,t))} \left[\lfloor z \rceil_{2p_1 d} \in t\mathbb{Z} + \left(-\frac{q}{(\log n)^2}, \frac{q}{(\log n)^2} \right) \right] + \mathrm{negl}(n) \leq \frac{1}{5} + \mathrm{negl}(n),
\end{aligned}$$

where (a) uses $q/t \in \mathbb{N}^+$; (b) uses Lemma 3.19 and the fact that applying rounding does not increase the statistical distance of the underlying distribution.

Then, since $\beta > \log(n) \in \omega(\sqrt{\log n})$, we have

$$\begin{aligned}
& \Pr_{y \leftarrow D_{\mathbb{Z},\beta}} \left[2p_1 d \cdot y \in q\mathbb{Z} + \left(-\frac{q}{(\log n)^2}, \frac{q}{(\log n)^2} \right) \right] \\
\leq_{(a)} \; & \Pr_{z \leftarrow D_{2p_1 d\beta}} \left[\lfloor z \rceil_{2p_1 d} \in q\mathbb{Z} + \left(-\frac{q}{(\log n)^2}, \frac{q}{(\log n)^2} \right) \right] + \mathrm{negl}(n) \leq_{(b)} \frac{1}{5} + \mathrm{negl}(n) < \frac{1}{4},
\end{aligned}$$

where (a) follows Lemma 3.18, (b) uses Eqn. (41). This concludes the proof of Claim 3.17. □

Therefore, the probability that

$$d \cdot [\mathbf{s}_{[\kappa \ldots \ell]}, \mathbf{e}] \in \left\{ \cup_{j \in \mathbb{Z}} ((j - 1/(\log n)^2)q, (j + 1/(\log n)^2)q) \right\}^{n-\kappa}$$

is smaller than $0.25^{n-\kappa}$. This concludes the proof of Claim 3.16. □

This concludes the proof of Claim 3.15. □

Therefore, with all but negligible probability, $\lambda_2^\infty\left(L_q^\perp(\mathbf{A})\right) \geq q/(\log n)^2$. This concludes the proof of Lemma 3.7. □

3.6.2 Detailed proofs in Step 3

Lemma 3.20. *For $|\varphi_3\rangle$, $|\varphi_3'\rangle$ defined in Eqn. (21), $|\varphi_3\rangle \approx_t |\varphi_3'\rangle$.*

Proof. Let $H \subset \mathbb{R}^{2n}$ be a lattice consisting of vectors $(\mathbf{z}_1^T, \mathbf{z}_2^T)^T$ such that $\mathbf{z}_1, \mathbf{z}_2 \in \mathbb{Z}^n$ and $\mathbf{z}_1 = \mathbf{z}_2 \bmod P$. We first observe that $|f_2(\mathbf{z})|$ (Eqn. (18)) is periodic in the following sense: define

$$L_{\mathbf{x}} := L_P^\perp(\mathbf{x}^T) =_{Eqn.\ (11)} \{\mathbf{z} \in \mathbb{Z}^n \mid \langle \mathbf{x}, \mathbf{z}\rangle \equiv 0 \bmod P\}. \tag{42}$$

Then, for any $\mathbf{c} \in \mathbb{Z}^n$, $|f_2(\mathbf{z})|$ is the same for all $\mathbf{z} \in L_{\mathbf{x}} + \mathbf{c}$, i.e., $|\{|f_2(\mathbf{z})| \mid \mathbf{z} \in L_{\mathbf{x}} + \mathbf{c}\}| = 1$. Denote $f_2^{max} := \max_{\mathbf{z}\in\mathbb{Z}^n}\left\{|f_2(\mathbf{z})|^2\right\}$, $\mathbf{z}_{max} := \arg\max_{\mathbf{z}\in\mathbb{Z}^n}\left\{|f_2(\mathbf{z})|^2\right\}$. Let $L_{\mathbf{x}} + \mathbf{c}_{max}$ be the coset of $L_{\mathbf{x}}$ where $\mathbf{z}_{max}$ is chosen from. Note that there exist multiple vectors $\mathbf{z}_{max}$, we just pick one of them. Same for $\mathbf{c}_{max}$.

Now we prove $|\varphi_3\rangle \approx_t |\varphi_3'\rangle$. If we treat $|\varphi_3\rangle$ and $|\varphi_3'\rangle$ as unnormalized vectors, then

$$\begin{aligned}
\||\varphi_3\rangle - |\varphi_3'\rangle\|_2^2 = & \sum_{\mathbf{z}_P\in\mathbb{Z}_P^n}\left|\sum_{\mathbf{z}\in P\cdot\mathbb{Z}^n+\mathbf{z}_P, \|\mathbf{z}-\mathbf{z}'\|_\infty \geq V\log n} f_2(\mathbf{z})\exp\left(-\pi\frac{t^2r^2s^2(s^2-r^2i)}{P^2u^2(s^4+r^4)}\|\mathbf{z}-\mathbf{z}'\|^2\right)\right|^2 \\
\leq_{(a)} & \sum_{\mathbf{z}_P\in\mathbb{Z}_P^n}\left(\sum_{\mathbf{z}\in P\cdot\mathbb{Z}^n+\mathbf{z}_P, \|\mathbf{z}-\mathbf{z}'\|_\infty \geq V\log n} |f_2(\mathbf{z})|\rho_V\left(\mathbf{z}-\mathbf{z}'\right)\right)^2 \\
\leq & f_2^{max}\cdot\sum_{\mathbf{z}_P\in\mathbb{Z}_P^n}\left(\sum_{\mathbf{z}\in P\cdot\mathbb{Z}^n+\mathbf{z}_P, \|\mathbf{z}-\mathbf{z}'\|_\infty \geq V\log n} \rho_V\left(\mathbf{z}-\mathbf{z}'\right)\right)^2 \\
=_{(b)} & f_2^{max}\cdot\sum_{\mathbf{z}_P\in\mathbb{Z}_P^n}\left(\sum_{\mathbf{z}^*\in P\cdot\mathbb{Z}^n+\mathbf{z}_P-\mathbf{z}', \|\mathbf{z}^*\|_\infty \geq V\log n} \rho_V\left(\mathbf{z}^*\right)\right)^2 \\
=_{(c)} & f_2^{max}\cdot\sum_{\mathbf{z}_P\in\mathbb{Z}_P^n}\left(\sum_{\mathbf{z}^*\in P\cdot\mathbb{Z}^n+\mathbf{z}_P, \|\mathbf{z}^*\|_\infty \geq V\log n} \rho_V\left(\mathbf{z}^*\right)\right)^2 \\
= & f_2^{max}\cdot\sum_{\mathbf{z}_P\in\mathbb{Z}_P^n}\left(\sum_{\mathbf{z}_1\in P\cdot\mathbb{Z}^n+\mathbf{z}_P, \|\mathbf{z}_1\|_\infty \geq V\log n} \rho_V\left(\mathbf{z}_1\right)\right)\left(\sum_{\mathbf{z}_2\in P\cdot\mathbb{Z}^n+\mathbf{z}_P, \|\mathbf{z}_2\|_\infty \geq V\log n} \rho_V\left(\mathbf{z}_2\right)\right) \\
= & f_2^{max}\cdot\sum_{\mathbf{z}_1,\mathbf{z}_2\in\mathbb{Z}^n, \mathbf{z}_1=\mathbf{z}_2 \bmod P, \|\mathbf{z}_1\|_\infty, \|\mathbf{z}_2\|_\infty \geq V\log n} \rho_V\left(\mathbf{z}_1\right)\rho_V\left(\mathbf{z}_2\right) \\
= & f_2^{max}\cdot\sum_{\mathbf{z}_H\in H, \|\mathbf{z}_H\|_\infty \geq V\log n} \rho_V(\mathbf{z}_H) \\
\leq_{Lemma\ 2.6} & f_2^{max}\cdot\mathrm{negl}(n)\cdot\rho_V(H),
\end{aligned} \tag{43}$$

where in (a) we drop all phase terms; in (b) we let $\mathbf{z}^* := \mathbf{z} - \mathbf{z}'$; in (c) we merge $-\mathbf{z}'$ into the support of $\mathbf{z}_P$.

To get a lower bound of $\left\| \left| \varphi_3' \right\rangle \right\|_2^2$, we start from

$$\begin{aligned} \left\| \left| \varphi_3' \right\rangle \right\|_2^2 &= \sum_{\mathbf{z} \in \mathbf{z}' + (\mathbb{Z}^n \cap V \log n \mathcal{B}_\infty^n)} |f_2(\mathbf{z})|^2 \rho_V^2(\mathbf{z} - \mathbf{z}') \\ &\geq f_2^{max} \sum_{\mathbf{z} \in L_{\mathbf{x}} + \mathbf{c}_{max} \cap (\mathbf{z}' + V \log n \mathcal{B}_\infty^n)} \rho_V^2(\mathbf{z} - \mathbf{z}') \\ &= f_2^{max} \sum_{\mathbf{z} \in L_{\mathbf{x}} + \mathbf{c}_{max} - \mathbf{z}' \cap V \log n \mathcal{B}_\infty^n} \rho_V^2(\mathbf{z}). \end{aligned} \tag{44}$$

To continue, we define $H_{\mathbf{x}} \subset \mathbb{R}^{2n}$ as a lattice consisting of vectors $(\mathbf{z}_1^T, \mathbf{z}_2^T)^T$ such that $\mathbf{z}_1, \mathbf{z}_2 \in L_{\mathbf{x}}$ and $\mathbf{z}_1 = \mathbf{z}_2 \bmod P$. For $L_{\mathbf{x}} = L_P^\perp(\mathbf{x}^T) \subset \mathbb{Z}^n$ defined in Eqn. (42), recall that $\mathbf{x} = D\mathbf{b}$. Therefore, $\frac{\det(H_{\mathbf{x}})}{\det(H)} = \frac{\det(L_{\mathbf{x}})}{\det(\mathbb{Z}^n)} = \frac{P}{D}$.

Next, we additionally observe that all cosets of $L_{\mathbf{x}}$, $L_{\mathbf{x}} + \mathbf{c}$, where $\mathbf{c} \in \mathbb{Z}^n$, have "short" representations in the following sense: we can set $\mathbf{c} = [c_1, 0, ..., 0]^T$ where $|c_1| \leq \frac{P}{2D}$ (this observation will be used in Eqn. (46), Step (b)). To wit, we observe that each $\mathbf{z} \in L_{\mathbf{x}} + \mathbf{c}$ satisfies $\langle \mathbf{x}, \mathbf{z} \rangle \equiv \langle \mathbf{x}, \mathbf{c} \rangle \equiv c^* \pmod P$ for some $c^* \in D\mathbb{Z} \cap [-P/2, P/2)$. Since the first coordinate of $\mathbf{x}$ is $-D$, we can use $L_{\mathbf{x}} - (c^*/D, 0, ..., 0)^T$ to represent $L_{\mathbf{x}} + \mathbf{c}$. Following this observation, we choose $\mathbf{c}' = (-c'/D, 0, ..., 0)^T$ where $c' = \langle \mathbf{c}_{max} - \mathbf{z}', \mathbf{x} \rangle \bmod P$. Therefore $L_{\mathbf{x}} + \mathbf{c}_{max} - \mathbf{z}' = L_{\mathbf{x}} + \mathbf{c}'$.

Let $\mathbf{c}'' := [\mathbf{c}'^T \mid \mathbf{c}'^T]^T$. We have

$$\begin{aligned} \left\| \left| \varphi_3' \right\rangle \right\|_2^2 &\geq_{Eqn.\ (44)} f_2^{max} \sum_{\mathbf{z} \in L_{\mathbf{x}} + \mathbf{c}' \cap V \log n \mathcal{B}_\infty^n} \rho_V^2(\mathbf{z}) \\ &= f_2^{max} \sum_{\mathbf{z}_1 \in L_{\mathbf{x}} + \mathbf{c}' \cap V \log n \mathcal{B}_\infty^n} \rho_V(\mathbf{z}_1) \left(\sum_{\mathbf{z}_2 \in L_{\mathbf{x}} + \mathbf{c}' \cap V \log n \mathcal{B}_\infty^n, \mathbf{z}_2 = \mathbf{z}_1 \bmod P} \rho_V(\mathbf{z}_2) \right) \\ &= f_2^{max} \sum_{\mathbf{z}_H \in H_{\mathbf{x}} + \mathbf{c}'' \cap V \log n \mathcal{B}_\infty^{2n}} \rho_V(\mathbf{z}_H) \\ &\geq_{Lemma\ 2.6} f_2^{max} \left(\sum_{\mathbf{z}_H \in H_{\mathbf{x}} + \mathbf{c}''} \rho_V(\mathbf{z}_H) - \mathrm{negl}(n) \cdot \rho_V(H_{\mathbf{x}}) \right) \\ &\geq_{H_{\mathbf{x}} \subset H} f_2^{max} \left(\sum_{\mathbf{z}_H \in H_{\mathbf{x}} + \mathbf{c}''} \rho_V(\mathbf{z}_H) - \mathrm{negl}(n) \cdot \rho_V(H) \right) \\ &\geq_{Eqn.\ (46)} f_2^{max} \cdot \frac{1}{\mathrm{poly}(n)} \cdot \rho_V(H). \end{aligned} \tag{45}$$

The last inequality in (45) is proven as follows

$$\begin{aligned}
&\sum_{\mathbf{z}_H \in H_{\mathbf{x}}+\mathbf{c}''} \rho_V(\mathbf{z}_H) \\
=_{PSF}\ & \frac{1}{\det(H_{\mathbf{x}})} \sum_{\mathbf{w}\in H^*_{\mathbf{x}}} \rho_{1/V}(\mathbf{w}) \cdot e^{2\pi i \langle \mathbf{c}'', \mathbf{w}\rangle} \\
=_{(a)}\ & \frac{D}{P\det(H)} \left(\sum_{\mathbf{w}\in H^*_{\mathbf{x}}, \|\mathbf{w}\|_\infty < \frac{\log n}{V}} \rho_{1/V}(\mathbf{w}) \cdot e^{2\pi i \langle \mathbf{c}'', \mathbf{w}\rangle} + \sum_{\mathbf{w}\in H^*_{\mathbf{x}}, \|\mathbf{w}\|_\infty \geq \frac{\log n}{V}} \rho_{1/V}(\mathbf{w}) \cdot e^{2\pi i \langle \mathbf{c}'', \mathbf{w}\rangle} \right) \\
\geq_{(b)}\ & \frac{D}{P\det(H)} \left(0.5 \cdot \sum_{\mathbf{w}\in H^*_{\mathbf{x}}, \|\mathbf{w}\|_\infty < \frac{\log n}{V}} \rho_{1/V}(\mathbf{w}) - \mathrm{negl}(n) \cdot \sum_{\mathbf{w}\in H^*_{\mathbf{x}}} \rho_{1/V}(\mathbf{w}) \right) \\
\geq_{(c)}\ & \frac{0.4D}{P\det(H)} \sum_{\mathbf{w}\in H^*_{\mathbf{x}}} \rho_{1/V}(\mathbf{w}) \\
\geq_{(d)}\ & \frac{0.4D}{P\det(H)} \sum_{\mathbf{w}\in H^*} \rho_{1/V}(\mathbf{w}) =_{PSF} \frac{0.4D}{P} \rho_V(H) \in \frac{1}{\mathrm{poly}(n)} \cdot \rho_V(H),
\end{aligned} \tag{46}$$

where in (a) we use $\det(H_{\mathbf{x}}) = \frac{P}{D} \cdot \det(H)$; in (b), the "$\|\mathbf{w}\|_\infty < \frac{\log n}{V}$" part uses $|\langle \mathbf{c}'', \mathbf{w}\rangle| < \frac{2P\log n}{2DV} < \frac{1}{20}$ for all $\mathbf{w} \in H^*_{\mathbf{x}}$ such that $\|\mathbf{w}\|_\infty < \frac{\log n}{V}$; the "$\|\mathbf{w}\|_\infty \geq \frac{\log n}{V}$" part uses Lemma 2.6; (c) uses Lemma 2.6 again to show that $\sum_{\mathbf{w}\in H^*_{\mathbf{x}}, \|\mathbf{w}\|_\infty < \frac{\log n}{V}} \rho_{1/V}(\mathbf{w}) \geq (1 - \mathrm{negl}(n)) \sum_{\mathbf{w}\in H^*_{\mathbf{x}}} \rho_{1/V}(\mathbf{w})$; (d) uses $H^* \subset H^*_{\mathbf{x}}$.

Therefore, combining Eqns. (43) and (45):

$$\left\| |\varphi_3\rangle - \left|\varphi_3'\right\rangle \right\|_2^2 \leq f_2^{max} \cdot \mathrm{negl}(n) \cdot \rho_V(H) \in \mathrm{negl}(n) \cdot \left\| \left|\varphi_3'\right\rangle \right\|_2^2.$$

Then $|\varphi_3\rangle \approx_t |\varphi_3'\rangle$ follows Lemma 2.11. □

Lemma 3.21. *For $\Sigma, \mathbf{d}_j, C_j$ defined in Eqn.* (23)*, $(Pj + \langle \mathbf{x}, \mathbf{z}\rangle)^2 + t^2\|\mathbf{z}-\mathbf{z}'\|^2 = (\mathbf{z}-\mathbf{d}_j)^T\Sigma^{-1}(\mathbf{z}-\mathbf{d}_j) + C_j$.*

Proof. We use the following formula:

Lemma 3.22. *For symmetric matrices Σ_1^{-1}, Σ_2^{-1}, and vectors $\mathbf{m}_1$, $\mathbf{m}_2$. Suppose $\Sigma_3^{-1} = \Sigma_1^{-1} + \Sigma_2^{-1}$ is invertible, then let $\mathbf{m}_3 = \Sigma_3(\Sigma_1^{-1}\mathbf{m}_1 + \Sigma_2^{-1}\mathbf{m}_2)$, $C = \mathbf{m}_1^T\Sigma_1^{-1}\mathbf{m}_1 + \mathbf{m}_2^T\Sigma_2^{-1}\mathbf{m}_2 - \mathbf{m}_3^T\Sigma_3^{-1}\mathbf{m}_3$. Then*

$$(\mathbf{v}-\mathbf{m}_1)^T\Sigma_1^{-1}(\mathbf{v}-\mathbf{m}_1) + (\mathbf{v}-\mathbf{m}_2)^T\Sigma_2^{-1}(\mathbf{v}-\mathbf{m}_2) = (\mathbf{v}-\mathbf{m}_3)^T\Sigma_3^{-1}(\mathbf{v}-\mathbf{m}_3) + C. \tag{47}$$

Proof.

$$\begin{aligned}
&(\mathbf{v}-\mathbf{m}_3)^T\Sigma_3^{-1}(\mathbf{v}-\mathbf{m}_3) - (\mathbf{v}-\mathbf{m}_1)^T\Sigma_1^{-1}(\mathbf{v}-\mathbf{m}_1) - (\mathbf{v}-\mathbf{m}_2)^T\Sigma_2^{-1}(\mathbf{v}-\mathbf{m}_2) \\
=_{(a)}\ & \mathbf{v}^T(\Sigma_1^{-1}+\Sigma_2^{-1})\mathbf{v} - 2\mathbf{v}^T(\Sigma_1^{-1}+\Sigma_2^{-1})\mathbf{m}_3 - \mathbf{v}^T\Sigma_1^{-1}\mathbf{v} - \mathbf{v}^T\Sigma_2^{-1}\mathbf{v} + 2\mathbf{v}^T\Sigma_1^{-1}\mathbf{m}_1 + 2\mathbf{v}^T\Sigma_2^{-1}\mathbf{m}_2 - C \\
=\ & -2\mathbf{v}^T(\Sigma_1^{-1}+\Sigma_2^{-1})\mathbf{m}_3 + 2\mathbf{v}^T\Sigma_1^{-1}\mathbf{m}_1 + 2\mathbf{v}^T\Sigma_2^{-1}\mathbf{m}_2 - C \\
=\ & -2\mathbf{v}^T(\Sigma_1^{-1}\mathbf{m}_1 + \Sigma_2^{-1}\mathbf{m}_2) + 2\mathbf{v}^T\Sigma_1^{-1}\mathbf{m}_1 + 2\mathbf{v}^T\Sigma_2^{-1}\mathbf{m}_2 - C \\
=\ & -C,
\end{aligned}$$

where (a) uses the fact that Σ_1^{-1} and Σ_2^{-1} are symmetric. □

We then apply Lemma 3.22 with $\mathbf{v} = \mathbf{z}$, $\mathbf{m}_1 = -\frac{Pj\mathbf{x}}{\|\mathbf{x}\|^2}$, $\mathbf{m}_2 = \mathbf{z}'$, $\Sigma_1^{-1} = \mathbf{x}\mathbf{x}^T$, $\Sigma_2^{-1} = t^2\mathbf{I}_n$. So $\Sigma_3^{-1} := t^2\mathbf{I}_n + \mathbf{x}\mathbf{x}^T$. From Formula (8) we get $\Sigma_3 = \frac{1}{t^2}\mathbf{I}_n - \frac{\frac{1}{t^4}\mathbf{x}\mathbf{x}^T}{1+\frac{1}{t^2}\|\mathbf{x}\|^2} = \frac{1}{t^2}\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{t^2+\|\mathbf{x}\|^2}\right)$. Then

$$\begin{aligned}
\mathbf{m}_3 =&\ \frac{1}{t^2}\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{t^2+\|\mathbf{x}\|^2}\right)(-\mathbf{x}Pj + t^2\mathbf{z}') = \frac{1}{t^2}\left(-\mathbf{x}Pj + t^2\mathbf{z}' + \frac{\mathbf{x}Pj\|\mathbf{x}\|^2}{t^2+\|\mathbf{x}\|^2} - \frac{\mathbf{x}t^2\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)\\
=&\ \mathbf{z}' - \frac{\mathbf{x}Pj}{t^2+\|\mathbf{x}\|^2} - \frac{\mathbf{x}\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2} = \mathbf{z}' - \mathbf{x}\frac{Pj+\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\\
\mathbf{m}_3^T\Sigma_3^{-1}\mathbf{m}_3 =&\ (\Sigma_1^{-1}\mathbf{m_1} + \Sigma_2^{-1}\mathbf{m_2})^T\cdot\mathbf{m}_3 = (-Pj\mathbf{x} + t^2\mathbf{z}')^T\cdot\left(\mathbf{z}' - \mathbf{x}\frac{Pj+\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)\\
=&\ t^2\|\mathbf{z}'\|^2 + \frac{Pj\|\mathbf{x}\|^2(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)}{t^2+\|\mathbf{x}\|^2} - \langle\mathbf{x},\mathbf{z}'\rangle\left(Pj + t^2\frac{Pj+\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right),
\end{aligned}$$

$$\begin{aligned}
C =&\ (Pj)^2 + t^2\|\mathbf{z}'\|^2 - t^2\|\mathbf{z}'\|^2 - \frac{Pj\|\mathbf{x}\|^2(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)}{t^2+\|\mathbf{x}\|^2} + \langle\mathbf{x},\mathbf{z}'\rangle\left(Pj + t^2\frac{Pj+\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)\\
=&\ (Pj)^2 - \frac{(Pj)^2\|\mathbf{x}\|^2}{t^2+\|\mathbf{x}\|^2} - \frac{Pj\|\mathbf{x}\|^2\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2} + \langle\mathbf{x},\mathbf{z}'\rangle Pj + \langle\mathbf{x},\mathbf{z}'\rangle\left(t^2\frac{Pj}{t^2+\|\mathbf{x}\|^2}\right) + \langle\mathbf{x},\mathbf{z}'\rangle\left(t^2\frac{\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)\\
=&\ \frac{t^2}{t^2+\|\mathbf{x}\|^2}(Pj)^2 + \frac{2Pj\langle\mathbf{x},\mathbf{z}'\rangle t^2}{t^2+\|\mathbf{x}\|^2} + \left(\frac{t^2\langle\mathbf{x},\mathbf{z}'\rangle^2}{t^2+\|\mathbf{x}\|^2}\right) = \frac{t^2}{t^2+\|\mathbf{x}\|^2}(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)^2.
\end{aligned}$$

Plugging in $\mathbf{d}_j = \mathbf{m}_3$, $C_j = C$ gives Lemma 3.21. □

3.6.3 Detailed proofs in Step 5: the distribution of $\mathbf{h}^*$

To understand the distribution of $\mathbf{h}^*$ obtained in Step 5, we first prove the expression of $|\varphi_4\rangle$ (cf. Eqn. (24)) can be written equivalently as follows:

Lemma 3.23. *If $\frac{s^2r^4}{\|\mathbf{x}\|^2(s^4+r^4)}\frac{t^2}{t^2+\|\mathbf{x}\|^2} \in 2\mathbb{Z}$ (implied by Cond. **C.5** which says $\frac{s^2r^4}{\|\mathbf{x}\|^2(s^4+r^4)}\frac{t^2}{t^2+\|\mathbf{x}\|^2} = 2(t^2+u^2) \in 2\mathbb{Z}$), then, let $\mathbf{w}_{\mathbf{h},\mathbf{m}} := \frac{\langle\mathbf{h}+\mathbf{m},\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} - \frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} + \frac{\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}$, we have*

$$\begin{aligned}
|\varphi_4\rangle = \sum_{\mathbf{h}\in\mathbb{Z}_P^n}\sum_{\mathbf{m}\in P\mathbb{Z}^n}&\exp\left(-\pi\frac{\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)^T\cdot\Sigma\cdot\left(\mathbf{h}+\mathbf{m}+\frac{\langle\mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)\right)\\
&\cdot e^{-2\pi i\frac{\left\langle\mathbf{z}'-\mathbf{x}\frac{\langle\mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\mathbf{h}+\mathbf{m}\right\rangle}{P}}\cdot\sum_{k\in\mathbb{Z}}e^{-\pi\frac{\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4r^2t^2}(k-\mathbf{w}_{\mathbf{h},\mathbf{m}})^2}\cdot e^{2\pi i\frac{\langle\mathbf{x},\mathbf{z}'\rangle}{P}(k-\mathbf{w}_{\mathbf{h},\mathbf{m}})}|\mathbf{h}\rangle.
\end{aligned}$$

Proof. We open the term in $\sum_{j\in\mathbb{Z}}$ in the expression of $|\varphi_4\rangle$ in Eqn. (24). First let us open $e^{-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}C_j}$:

$$\begin{aligned}
&\exp\left(-\pi\frac{s^2r^2(s^2-r^2i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\frac{t^2}{t^2+\|\mathbf{x}\|^2}(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)^2\right)\\
=&\ \exp\left(-\pi\frac{s^4r^2}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\frac{t^2}{t^2+\|\mathbf{x}\|^2}(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)^2\right)\exp\left(\pi\frac{s^2r^4i}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\frac{t^2}{t^2+\|\mathbf{x}\|^2}(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)^2\right)\\
=_{(a)}&\ \exp\left(-\pi\frac{s^4r^2}{P^2\|\mathbf{x}\|^2(s^4+r^4)}\frac{t^2}{t^2+\|\mathbf{x}\|^2}(Pj+\langle\mathbf{x},\mathbf{z}'\rangle)^2\right)\exp\left(2\pi i\frac{t^2+\|\mathbf{x}\|^2}{P^2}(2Pj\langle\mathbf{x},\mathbf{z}'\rangle+\langle\mathbf{x},\mathbf{z}'\rangle^2)\right),
\end{aligned}$$

where (a) holds given $j \in \mathbb{Z}$ and Condition **C.5** which says $\frac{s^2r^4}{\|\mathbf{x}\|^2(s^4+r^4)} \frac{t^2}{t^2+\|\mathbf{x}\|^2} = 2(t^2+\|\mathbf{x}\|^2) \in 2\mathbb{Z}$, so we can delete the $(Pj)^2$ term in the imaginary part.
Therefore, the term in $\sum_{j\in\mathbb{Z}}$ in the expression of $|\varphi_4\rangle$ equals to

$$
\begin{aligned}
& \sum_{j\in\mathbb{Z}} e^{-2\pi i \frac{\left\langle \mathbf{d}_j, \mathbf{h}+\mathbf{m}+\frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right\rangle}{P}} \cdot e^{-2\pi i \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} j} \cdot e^{-\pi \frac{s^2r^2(s^2-r^2 i)}{P^2\|\mathbf{x}\|^2(s^4+r^4)} C_j} \\
\propto_{(a)} \quad & \sum_{j\in\mathbb{Z}} e^{-2\pi i \frac{\left\langle \mathbf{z}' - \mathbf{x}\frac{Pj+\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}, \mathbf{h}+\mathbf{m}+\frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right\rangle}{P}} \cdot e^{-2\pi i \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} j} \cdot e^{-\pi \frac{s^4r^2}{P^2\|\mathbf{x}\|^2(s^4+r^4)} \frac{t^2}{t^2+\|\mathbf{x}\|^2} (Pj+\langle \mathbf{x},\mathbf{z}'\rangle)^2} \cdot e^{2\pi i \frac{(t^2+\|\mathbf{x}\|^2)\cdot 2Pj\langle \mathbf{x},\mathbf{z}'\rangle}{P^2}} \\
= \quad & e^{-2\pi i \frac{\left\langle \mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}, \mathbf{h}+\mathbf{m}+\frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right\rangle}{P}} \\
& \cdot \sum_{j\in\mathbb{Z}} e^{2\pi i \left\langle \frac{\mathbf{x}}{t^2+\|\mathbf{x}\|^2}, \mathbf{h}+\mathbf{m}+\frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right\rangle \cdot j} \cdot e^{-2\pi i \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} j} \cdot e^{-\pi \frac{s^4r^2t^2}{\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)} \left(j+\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{P}\right)^2} \cdot e^{2\pi i \frac{2(t^2+\|\mathbf{x}\|^2)\langle \mathbf{x},\mathbf{z}'\rangle \cdot j}{P}} \\
\propto_{(b)} \quad & e^{-2\pi i \frac{\left\langle \mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}, \mathbf{h}+\mathbf{m} \right\rangle}{P}} \cdot \sum_{k\in\mathbb{Z}} e^{-\pi \frac{\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4r^2t^2} (k-\mathbf{w}_{\mathbf{h},\mathbf{m}})^2} \cdot e^{2\pi i \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{P}(k-\mathbf{w}_{\mathbf{h},\mathbf{m}})},
\end{aligned}
$$

where $\propto_{(a)}$ omits the global phase of $e^{2\pi i \frac{t^2+\|\mathbf{x}\|^2}{P^2}\langle \mathbf{x},\mathbf{z}'\rangle^2}$; $\propto_{(b)}$ uses PSF from $\sum_{j\in\mathbb{Z}}$ to $\sum_{k\in\mathbb{Z}}$, and omits the global phase of $e^{-2\pi i \frac{\left\langle \mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}, \frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right\rangle}{P}}$; $\mathbf{w}_{\mathbf{h},\mathbf{m}}$ equals to

$$
\mathbf{w}_{\mathbf{h},\mathbf{m}} = \frac{\langle \mathbf{h}+\mathbf{m},\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} + \frac{2(t^2+\|\mathbf{x}\|^2)\langle \mathbf{x},\mathbf{z}'\rangle}{P} =_{\mathbf{C.5},\mathbf{C.2}} \frac{\langle \mathbf{h}+\mathbf{m},\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2} \tag{48}
$$

□

Lemma 3.24. *With probability* $1-2^{-\Omega(n)}$*, the vector* $\mathbf{h}^* \in \mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2}$ *obtained from the measurement in Step 5 satisfies* $\operatorname{dist}\left(\frac{\langle \mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}, \mathbb{Z}\right) \le \frac{2ut^2}{r}\sqrt{n}\log n$.

Proof. Recall that $\mathbf{h} = \mathbf{h}'(t^2+\|\mathbf{x}\|^2) + \mathbf{h}''$, so $|\varphi_4\rangle$ can be equivalently written as

$$
\begin{aligned}
|\varphi_4\rangle = \sum_{\mathbf{h}'\in\mathbb{Z}^n_M} \sum_{\mathbf{h}''\in\mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2}} \sum_{\mathbf{m}\in P\mathbb{Z}^n} & e^{-\pi \frac{\|\mathbf{x}\|^2(s^2+r^2 i)}{s^2r^2} \left(\mathbf{h}'(t^2+\|\mathbf{x}\|^2)+\mathbf{m}+\mathbf{h}''+\frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)^T \cdot \Sigma \cdot \left(\mathbf{h}'(t^2+\|\mathbf{x}\|^2)+\mathbf{m}+\mathbf{h}''+\frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)} \\
& \cdot \sum_{k\in\mathbb{Z}} e^{-\pi \frac{\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4r^2t^2} \left(k-\mathbf{w}_{\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}'',\mathbf{m}}\right)^2} \cdot e^{2\pi i \phi_5(\mathbf{h}',\mathbf{h}'',\mathbf{m},k)} \left|\mathbf{h}'\right\rangle \left|\mathbf{h}''\right\rangle,
\end{aligned} \tag{49}
$$

where $e^{2\pi i \phi_5(\mathbf{h}',\mathbf{h}'',\mathbf{m},k)} = e^{-2\pi i \frac{\left\langle \mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}, \mathbf{h}'(t^2+\|\mathbf{x}\|^2)+\mathbf{m}+\mathbf{h}'' \right\rangle}{P}} \cdot e^{2\pi i \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{P}\left(k-\mathbf{w}_{\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}'',\mathbf{m}}\right)}$.
To understand how $|\varphi_5\rangle$ looks like, let us take a closer look in the terms inside $\sum_{k\in\mathbb{Z}}$. Note that $k - \mathbf{w}_{\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}'',\mathbf{m}} = k - \langle \mathbf{h}',\mathbf{x}\rangle - \frac{\langle \mathbf{m},\mathbf{x}\rangle+\langle \mathbf{h}'',\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}$. So for all $\mathbf{h}' \in \mathbb{Z}^n_M, \mathbf{m} \in P\mathbb{Z}^n$, we

have $\langle \mathbf{h}', \mathbf{x} \rangle \in \mathbb{Z}$, $\frac{\langle \mathbf{m}, \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} \in M\mathbb{Z} \subset \mathbb{Z}$. Therefore

$$\begin{aligned}
&\sum_{k\in\mathbb{Z}} e^{-\pi \frac{\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4r^2t^2}\left(k-\mathbf{w}_{\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}'',\mathbf{m}}\right)^2} \cdot e^{2\pi i \frac{\langle \mathbf{x},\mathbf{z}' \rangle}{P}\left(k-\mathbf{w}_{\mathbf{h}'\cdot(t^2+\|\mathbf{x}\|^2)+\mathbf{h}'',\mathbf{m}}\right)} \\
&= \sum_{k'\in\mathbb{Z}} e^{-\pi \frac{\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4r^2t^2}\left(k'-\frac{\langle \mathbf{h}'',\mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2}+\frac{\langle \mathbf{x},\mathbf{y} \rangle}{\|\mathbf{x}\|^2}-\frac{\langle \mathbf{x},\mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2}\right)^2} \cdot e^{2\pi i \frac{\langle \mathbf{x},\mathbf{z}' \rangle}{P}\left(k'-\frac{\langle \mathbf{h}'',\mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2}+\frac{\langle \mathbf{x},\mathbf{y} \rangle}{\|\mathbf{x}\|^2}-\frac{\langle \mathbf{x},\mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2}\right)},
\end{aligned} \tag{50}$$

where the $k - \langle \mathbf{h}', \mathbf{x} \rangle - \frac{\langle \mathbf{m}, \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} \in \mathbb{Z}$ term is absorbed by $k' \in \mathbb{Z}$ (this provides another proof that the second line of the expression of $|\varphi_4\rangle$ of Eqn. (49) is independent of $\mathbf{h}'$ – the first proof is given in the paragraph after Eqn. (25)). Therefore, $|\varphi_4\rangle$ in Eqn. (50) can be equivalently written as

$$|\varphi_4\rangle = \sum_{\mathbf{h}'\in\mathbb{Z}_M^n} \sum_{\mathbf{h}''\in\mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2}} f_4(\mathbf{h}', \mathbf{h}'') \, |\mathbf{h}'\rangle \, |\mathbf{h}''\rangle = \sum_{\mathbf{h}'\in\mathbb{Z}_M^n} \sum_{\mathbf{h}''\in\mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2}} A(\mathbf{h}', \mathbf{h}'') \cdot B(\mathbf{h}', \mathbf{h}'') \, |\mathbf{h}'\rangle \, |\mathbf{h}''\rangle \,, \tag{51}$$

where

$$\begin{aligned}
A(\mathbf{h}', \mathbf{h}'') &:= \sum_{\mathbf{m}\in P\mathbb{Z}^n} e^{-\pi \frac{\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}'(t^2+\|\mathbf{x}\|^2)+\mathbf{m}+\mathbf{h}''+\frac{\langle \mathbf{x},\mathbf{y} \rangle \mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)^T \cdot \Sigma \cdot \left(\mathbf{h}'(t^2+\|\mathbf{x}\|^2)+\mathbf{m}+\mathbf{h}''+\frac{\langle \mathbf{x},\mathbf{y} \rangle \mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}\right)} \\
&\qquad \cdot e^{-2\pi i \frac{\left\langle \mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2}, \mathbf{h}'(t^2+\|\mathbf{x}\|^2)+\mathbf{m}+\mathbf{h}'' \right\rangle}{P}}, \\
B(\mathbf{h}', \mathbf{h}'') &:= \sum_{k'\in\mathbb{Z}} e^{-\pi \frac{\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4r^2t^2}\left(k'-\frac{\langle \mathbf{h}'',\mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2}+\frac{\langle \mathbf{x},\mathbf{y} \rangle}{\|\mathbf{x}\|^2}-\frac{\langle \mathbf{x},\mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2}\right)^2} \cdot e^{2\pi i \frac{\langle \mathbf{x},\mathbf{z}' \rangle}{P}\left(k'-\frac{\langle \mathbf{h}'',\mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2}+\frac{\langle \mathbf{x},\mathbf{y} \rangle}{\|\mathbf{x}\|^2}-\frac{\langle \mathbf{x},\mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2}\right)}.
\end{aligned}$$

To understand the distribution of $\mathbf{h}^*$ obtained by measuring $|\mathbf{h}''\rangle$, we observe that the width of the Gaussian function for the variable $\frac{\langle \mathbf{h}'', \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2}$ in Eqn. (50) is less than $\frac{rts^2}{ur^2t} = \frac{s^2}{ur} \leq_{\mathbf{C.5}} \frac{2u^2t^2}{ur} \cdot \left(1 + \frac{1}{\log n}\right) = \frac{2ut^2}{r} \cdot \left(1 + \frac{1}{\log n}\right) <_{\mathbf{C.7}} \frac{1}{4\beta\sqrt{n}\log^2 n} \cdot \left(1 + \frac{1}{\log n}\right) \ll 1$, whereas the width of the Gaussian function for the variable $\mathbf{h}''$ in the first line of Eqn. (49) is roughly $\frac{r}{u} \gg 1$. So the tail bound of $\mathbf{h}^*$ is almost determined by the second line of Eqn. (49).

Define the set $\mathcal{S}_{h''} := \left\{ \mathbf{h}'' \in \mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2} \,\middle|\, \mathrm{dist}\left(\frac{\langle \mathbf{h}'', \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x}, \mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2}, \mathbb{Z}\right) > \frac{2ut^2}{r}\sqrt{n}\log n \right\}$. We can split $|\varphi_4\rangle$ in Eqn. (51) as

$$|\varphi_4\rangle = \underbrace{\sum_{\mathbf{h}'\in\mathbb{Z}_M^n} \sum_{\mathbf{h}''\in\mathcal{S}_{h''}} f_4(\mathbf{h}', \mathbf{h}'') \left|\mathbf{h}'\right\rangle \left|\mathbf{h}''\right\rangle}_{=:\left|\varphi_4^*\right\rangle} + \underbrace{\sum_{\mathbf{h}'\in\mathbb{Z}_M^n} \sum_{\mathbf{h}''\in\mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2}\setminus\mathcal{S}_{h''}} f_4(\mathbf{h}', \mathbf{h}'') \left|\mathbf{h}'\right\rangle \left|\mathbf{h}''\right\rangle}_{=:\left|\varphi_4^{**}\right\rangle}$$

We prove Lemma 3.24 by showing that $\||\varphi_4^*\rangle\|_2^2 \in 2^{-\Omega(n)} \cdot \||\varphi_4^{**}\rangle\|_2^2$.

Claim 3.25. $\||\varphi_4^{**}\rangle\|_2^2 \geq \frac{1}{10}$.

Proof. It suffices to show there exists $\mathbf{h}' \in \mathbb{Z}_M^n, \mathbf{h}'' \in \mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2} \setminus \mathcal{S}_{h''}$ such that $|f_4(\mathbf{h}', \mathbf{h}'')|^2 \geq \frac{1}{10}$.

Consider the following set $\mathcal{T}$:

$$\mathcal{T} := \left\{ \mathbf{h}' \in \mathbb{Z}_M^n, \mathbf{h}'' \in \mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2} \,\middle|\, \mathbf{h}' \cdot (t^2 + \|\mathbf{x}\|^2) + \mathbf{h}'' = \mathbf{y} - \left\lfloor \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} \mathbf{x} \right\rceil + a|0^{n-1} \text{ where } |a| \leq \frac{t^2 + \|\mathbf{x}\|^2}{D} \right\}.$$

Since the first entry of $\mathbf{x}$ is $-D$, we know there exists $(\mathbf{h}', \mathbf{h}'') \in \mathcal{T}$ such that $\frac{\langle \mathbf{h}'', \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x}, \mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2} \in \mathbb{Z}$, hence $\mathbf{h}'' \in \mathbb{Z}^n_{t^2+\|\mathbf{x}\|^2} \setminus \mathcal{S}_{h''}$. For such a pair of $\mathbf{h}', \mathbf{h}''$, the absolute value of its amplitude can be analyzed as follows. First, for the B part of Eqn. (51), we have

$$|B(\mathbf{h}', \mathbf{h}'')| \geq 1 - \sum_{k' \in \mathbb{Z}, \left| k' - \frac{\langle \mathbf{h}'', \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2} \right| \geq 1} e^{-\pi \frac{\|\mathbf{x}\|^2 (s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4 r^2 t^2} \left(k' - \frac{\langle \mathbf{h}'', \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2} \right)^2} \geq_{(a)} 1 - \mathrm{negl}(n),$$

where (a) uses $\frac{s^2 r t}{\|\mathbf{x}\| \sqrt{(s^4+r^4)(t^2+\|\mathbf{x}\|^2)}} \leq_{\mathbf{C.5}} \frac{3ut^2}{r} \leq_{\mathbf{C.7}} \frac{1}{\log n}$ and Lemma 2.6.

Second, for the A part of Eqn. (51), we have

$$\begin{aligned} |A(\mathbf{h}', \mathbf{h}'')| &\geq_{(a)} e^{-\pi \frac{\|\mathbf{x}\|^2}{r^2 t^2} (\sqrt{n} + (t^2+\|\mathbf{x}\|^2)/D)^2} - \sum_{\mathbf{m} \in P\mathbb{Z}^n, \mathbf{m} \neq \mathbf{0}} e^{-\pi \frac{\|\mathbf{x}\|^2}{r^2 (t^2+\|\mathbf{x}\|^2)} \left\| \mathbf{h}'(t^2+\|\mathbf{x}\|^2) + \mathbf{m} + \mathbf{h}'' + \frac{\langle \mathbf{x}, \mathbf{y} \rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right\|^2} \\ &\geq_{(b)} 1/2 - \rho_{\frac{r\sqrt{t^2+\|\mathbf{x}\|^2}}{P\|\mathbf{x}\|}}(\mathbb{Z}^n) \cdot \mathrm{negl}(n) \geq_{(c)} 1/3, \end{aligned} \tag{52}$$

where (a) uses $\Sigma = \frac{1}{t^2} \left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{t^2+\|\mathbf{x}\|^2} \right)$ (from Eqn. (23)) and the fact that the eigenvalues of Σ are $\frac{1}{t^2}$ and $\frac{1}{t^2} \frac{t^2}{t^2+\|\mathbf{x}\|^2}$; (b) uses $e^{-\pi \frac{\|\mathbf{x}\|^2}{r^2 t^2} (\sqrt{n} + (t^2+\|\mathbf{x}\|^2)/D)^2} \geq 1/2$, and $\frac{r\sqrt{t^2+\|\mathbf{x}\|^2}}{P\|\mathbf{x}\|} =_{\mathbf{C.2}} \frac{r}{2(t^2+\|\mathbf{x}\|^2)^{1.5} u} < \frac{r}{ut^3} <_{\mathbf{C.7}} \frac{1}{\log n}$ and Lemma 2.6; (c) uses $\rho_{\frac{r\sqrt{t^2+\|\mathbf{x}\|^2}}{P\|\mathbf{x}\|}}(\mathbb{Z}^n) < 2$. Therefore, $\| |\varphi_4^{**}\rangle \|_2^2 \geq |AB|^2 \geq (1 - \mathrm{negl}(n))^2 (1/3)^2 \geq 1/10$. This completes the proof of Claim 3.25. □

Claim 3.26. $\| |\varphi_4^*\rangle \|_2^2 \leq 2^{-\Omega(n \log^2 n)}$.

Proof. For any $(\mathbf{h}', \mathbf{h}'') \in \mathbb{Z}_M^n \times \mathcal{S}_{h''}$, the absolute value of the amplitude on $|\mathbf{h}'\rangle |\mathbf{h}''\rangle$ is

$$\begin{aligned} &|A(\mathbf{h}', \mathbf{h}'') B(\mathbf{h}', \mathbf{h}'')| \\ \leq_{(a)} &\sum_{\mathbf{m} \in P\mathbb{Z}^n} e^{-\pi \frac{\|\mathbf{x}\|^2}{r^2} \left(\mathbf{h}'(t^2+\|\mathbf{x}\|^2) + \mathbf{m} + \mathbf{h}'' + \frac{\langle \mathbf{x}, \mathbf{y} \rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right)^T \cdot \Sigma \cdot \left(\mathbf{h}'(t^2+\|\mathbf{x}\|^2) + \mathbf{m} + \mathbf{h}'' + \frac{\langle \mathbf{x}, \mathbf{y} \rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right)} \cdot \sum_{k' \in \mathbb{Z}} e^{-\pi \frac{r^2}{9u^2 t^4} \left(k' - \frac{\langle \mathbf{h}'', \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2} \right)^2} \\ \leq_{(b)} &\sum_{\mathbf{m} \in P\mathbb{Z}^n} e^{-\pi \frac{\|\mathbf{x}\|^2}{r^2 (t^2+\|\mathbf{x}\|^2)} \left\| \mathbf{h}'(t^2+\|\mathbf{x}\|^2) + \mathbf{m} + \mathbf{h}'' + \frac{\langle \mathbf{x}, \mathbf{y} \rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y} \right\|^2} \cdot 2^{-\Omega(n \log^2 n)} \\ \leq &\ \rho_{\frac{r\sqrt{t^2+\|\mathbf{x}\|^2}}{P\|\mathbf{x}\|}}(\mathbb{Z}^n) \cdot 2^{-\Omega(n \log^2 n)} \in_{(c)} 2^{-\Omega(n \log^2 n)}, \end{aligned}$$

where in (a) we use $\frac{\|\mathbf{x}\|^2 (s^4+r^4)(t^2+\|\mathbf{x}\|^2)}{s^4 r^2 t^2} \geq \frac{r^2}{9u^2 t^4}$; in (b), $\sum_{k' \in \mathbb{Z}} e^{-\pi \frac{r^2}{9u^2 t^4} \left(k' - \frac{\langle \mathbf{h}'', \mathbf{x} \rangle}{t^2+\|\mathbf{x}\|^2} + \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x}, \mathbf{z}' \rangle}{t^2+\|\mathbf{x}\|^2} \right)^2} \leq 2^{-\Omega(n \log^2 n)} \cdot \rho_{\frac{3ut^2}{r}}(\mathbb{Z}) \leq 2^{-\Omega(n \log^2 n)}$ follows from $\mathbf{h}'' \in \mathcal{S}_{h''}$ and Lemma 2.5 over $k' \in \mathbb{Z}$; the rest of the expression under $\sum_{\mathbf{m} \in P\mathbb{Z}^n}$ uses $\Sigma = \frac{1}{t^2} \left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{t^2+\|\mathbf{x}\|^2} \right)$ (from Eqn. (23)) and the fact that the eigenvalues of Σ are $\frac{1}{t^2}$ and $\frac{1}{t^2} \frac{t^2}{t^2+\|\mathbf{x}\|^2}$; (c) uses $\rho_{\frac{r\sqrt{t^2+\|\mathbf{x}\|^2}}{P\|\mathbf{x}\|}}(\mathbb{Z}^n) < 2$ (same as Item (c) in Eqn. (52)).

Therefore, $\| |\varphi_4^*\rangle \|_2^2 \leq 2^{-\Omega(n \log^2 n)} \cdot P^n \in 2^{-\Omega(n \log^2 n)}$. □

Then Lemma 3.24 follows from Claims 3.25 and 3.26. □

3.6.4 Detailed proofs in Step 6

The entire §3.6.4 is devoted to proving that $|\varphi_6\rangle$ is negligibly close to $|\varphi_6'''\rangle$ in Eqn. (27). We first give the Fourier transformation calculation in Lemma 3.27, then prove tail bounds in Lemma 3.29.

Lemma 3.27. *For any* $\mathbf{c} \in \mathbb{Z}^n$, *let* $\mathbf{c}' := \mathbf{c} + \mathbf{z}' + \mathbf{h}^* - \mathbf{y} + \mathbf{x}\left(\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)$. *Then* $|\varphi_6\rangle = \sum_{\mathbf{c}\in\mathbb{Z}_M^n} f_6(\mathbf{c})\,|\mathbf{c}\rangle$ *where* $f_6 : \mathbb{Z}^n \to \mathbb{C}$ *satisfies: for any* $\mathbf{c} \in \mathbb{Z}^n$,

$$
\begin{aligned}
f_6(\mathbf{c}) = \sum_{\mathbf{k_c}\in 0|\mathbb{Z}^{n-1}} & e^{-\pi \frac{\left\|\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right)\right\|^2}{\sigma^2}} e^{2\pi i \mathbf{k_c}^T \cdot \frac{\mathbf{c}+\mathbf{z}'-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}}{M}} \cdot e^{-2\pi i \frac{\left\|\mathbf{c}+\mathbf{z}'-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}\right\|^2}{M^2}} \\
& \cdot \sum_{j\in\mathbb{Z}} e^{-\pi \frac{1}{\sigma_x^2}\left\|2Dj\mathbf{x} - \left(\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\mathbf{x}\right\|^2} \\
& \cdot e^{-2\pi i\left(\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{M\|\mathbf{x}\|^2}\left(2Dj - \left(\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right) + \frac{t^2}{M^2}\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle^2}{\|\mathbf{x}\|^4}\right)},
\end{aligned}
$$

where $\sigma_x \in \mathbb{C}$ *satisfies* $Re\left(\frac{1}{\sigma_x^2}\right) \in \frac{1}{\sigma^2}\cdot(1,3)$.

Note that in the proof we give a more accurate expression of $\frac{1}{\sigma_x^2} = \frac{1}{W+U''i}\frac{1}{(2D\|\mathbf{x}\|)^2}$ where W, U'' are defined in Eqns. (70), (64), but the loose bound of $Re\left(\frac{1}{\sigma_x^2}\right) \in \frac{1}{\sigma^2}\cdot(1,3)$ suffices for our purpose.

Proof. For $|\varphi_6\rangle = \mathsf{QFT}_{\mathbb{Z}_M^n}|\varphi_5\rangle$, where $|\varphi_5\rangle$ is defined in Eqn. (26), we have

$$
\begin{aligned}
|\varphi_6\rangle = & \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{h}'\in\mathbb{Z}_M^n}\sum_{\mathbf{m}\in P\mathbb{Z}^n} e^{-\pi\frac{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)^T\cdot\Sigma\cdot\left(\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)} \\
& \cdot e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'+\frac{\mathbf{m}+\mathbf{h}^*}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle}\cdot e^{-2\pi i\left\langle \mathbf{c},\frac{\mathbf{h}'}{M}\right\rangle}|\mathbf{c}\rangle \\
=_{(a)} & \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{h}'\in\mathbb{Z}_M^n}\sum_{\mathbf{m}\in P\mathbb{Z}^n} e^{-\pi\frac{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)^T\cdot\Sigma\cdot\left(\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)} \\
& \cdot e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle}\cdot e^{-2\pi i\left\langle \mathbf{c},\frac{\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle}|\mathbf{c}\rangle \\
=_{(b)} & \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{h}'\in\mathbb{Z}^n} e^{-\pi\frac{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^2+r^2i)}{s^2r^2}\left(\mathbf{h}'+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)^T\cdot\Sigma\cdot\left(\mathbf{h}'+\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\right)}\cdot e^{-2\pi i\frac{\left\langle \mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\mathbf{h}'\right\rangle}{M}}|\mathbf{c}\rangle,
\end{aligned}
$$

where in (a) we use $e^{-2\pi i\left\langle \mathbf{c},\frac{\mathbf{h}'}{M}\right\rangle} = e^{-2\pi i\left\langle \mathbf{c},\frac{\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle}$ since $\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2} \in M\mathbb{Z}^n$, and we omit the global phase of $e^{-2\pi i\left\langle \mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2},\frac{\mathbf{h}^*}{P}\right\rangle}$; in (b) we merge $\mathbf{h}'+\frac{\mathbf{m}}{t^2+\|\mathbf{x}\|^2}$ for $\mathbf{h}' \in \mathbb{Z}_M^n, \mathbf{m} \in P\mathbb{Z}^n$ into $\mathbf{h}' \in \mathbb{Z}^n$.

To continue analyzing $|\varphi_6\rangle$, recall from Eqn. (23) that $\Sigma = \frac{1}{t^2}\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{t^2+\|\mathbf{x}\|^2}\right)$, $\Sigma^{-1} = t^2\mathbf{I}_n + \mathbf{x}\mathbf{x}^T$. So by applying PSF from $\sum_{\mathbf{h}'\in\mathbb{Z}^n}$ to $\sum_{\mathbf{j}\in\mathbb{Z}^n}$, we get

$$|\varphi_6\rangle = \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{j}\in\mathbb{Z}^n} e^{-\pi\frac{s^2r^2(s^2-r^2i)}{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)^T\cdot\left(t^2\mathbf{I}_n+\mathbf{x}\mathbf{x}^T\right)\cdot\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)} \cdot e^{2\pi i\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)}|\mathbf{c}\rangle$$

Since $\frac{s^2r^4}{\|\mathbf{x}\|^2(s^4+r^4)}\frac{t^2}{(t^2+\|\mathbf{x}\|^2)^2} = 2$ (Condition **C.5**), we have for all $\mathbf{j} \in \mathbb{Z}^n$,

$$e^{\pi\frac{s^2r^4i}{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}\cdot t^2\left\|\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right\|^2} = e^{2\pi i\left(2\left\langle \mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M},\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle-\frac{\left\|\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right\|^2}{M^2}\right)}.$$

In other words, this enables us to erase the quadratic terms of $\mathbf{j}$ related to the imaginary part of the $\frac{s^2r^2(s^2-r^2i)}{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}t^2\mathbf{I}_n$ term in $\frac{s^2r^2(s^2-r^2i)}{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}\left(t^2\mathbf{I}_n+\mathbf{x}\mathbf{x}^T\right)$. Therefore,

$$\begin{aligned}
&e^{-\pi\frac{s^2r^2(s^2-r^2i)}{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)^T\cdot\left(t^2\mathbf{I}_n+\mathbf{x}\mathbf{x}^T\right)\cdot\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)}\\
=\ &e^{-\pi\frac{s^2r^2}{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)^T\cdot\left(s^2t^2\mathbf{I}_n+(s^2-r^2i)\mathbf{x}\mathbf{x}^T\right)\cdot\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)}\\
&\cdot e^{2\pi i\left(2\left\langle \mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M},\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle-\frac{\left\|\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right\|^2}{M^2}\right)}
\end{aligned}$$

Let $R := s^2t^2$, $T := s^2 - r^2i$. Then

$$\begin{aligned}
\left(R\mathbf{I}_n + T\mathbf{x}\mathbf{x}^T\right)^{-1} &= T^{-1}\cdot\left(\frac{R}{T}\mathbf{I}_n + \mathbf{x}\mathbf{x}^T\right)^{-1} =_{Eqn.\ (8)} \frac{1}{T}\cdot\left(\frac{T}{R}\mathbf{I}_n - \frac{\frac{T^2}{R^2}\mathbf{x}\mathbf{x}^T}{1+\frac{T}{R}\|\mathbf{x}\|^2}\right)\\
&= \left(\frac{1}{R}\mathbf{I}_n - \frac{\frac{T}{R^2}\mathbf{x}\mathbf{x}^T}{1+\frac{T}{R}\|\mathbf{x}\|^2}\right) = \frac{1}{R}\cdot\left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right).
\end{aligned} \tag{53}$$

Therefore, let $\mathbf{w}_{\mathbf{c},\mathbf{k}} := \mathbf{k} - \frac{\mathbf{h}^* + \frac{\langle \mathbf{x},\mathbf{y}\rangle \mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y}}{t^2+\|\mathbf{x}\|^2} - 2\frac{\mathbf{c}+\mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}$, $\theta_{\mathbf{c},\mathbf{k}} := \mathbf{k}^T \cdot \frac{\mathbf{c}+\mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M} - \frac{\left\|\mathbf{c}+\mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right\|^2}{M^2}$,

$$
\begin{aligned}
|\varphi_6\rangle = & \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{j}\in\mathbb{Z}^n} e^{-\pi\frac{s^2r^2}{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)^T\cdot\left(s^2t^2\mathbf{I}_n+(s^2-r^2i)\mathbf{x}\mathbf{x}^T\right)\cdot\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)} \\
& \cdot e^{2\pi i\left(2\left\langle \mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M},\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right\rangle - \frac{\left\|\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right\|^2}{M^2}\right)} \cdot e^{2\pi i\frac{\mathbf{h}^*+\frac{\langle \mathbf{x},\mathbf{y}\rangle\mathbf{x}}{\|\mathbf{x}\|^2}-\mathbf{y}}{t^2+\|\mathbf{x}\|^2}\left(\mathbf{j}+\frac{\mathbf{c}+\mathbf{z}'-\mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}}{M}\right)}|\mathbf{c}\rangle \\
=_{(a)} & \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{k}\in\mathbb{Z}^n} e^{-\pi\frac{(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}{s^2r^2}\mathbf{w}_{\mathbf{c},\mathbf{k}}^T\cdot\frac{1}{R}\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\mathbf{w}_{\mathbf{c},\mathbf{k}}}\cdot e^{2\pi i\theta_{\mathbf{c},\mathbf{k}}}|\mathbf{c}\rangle \\
= & \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{k}\in\mathbb{Z}^n} e^{-\pi\frac{2^2(t^2+\|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2(s^4+r^4)}{s^2r^2RM^2}\left(\frac{M}{2}\mathbf{w}_{\mathbf{c},\mathbf{k}}\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\frac{M}{2}\mathbf{w}_{\mathbf{c},\mathbf{k}}\right)}\cdot e^{2\pi i\theta_{\mathbf{c},\mathbf{k}}}|\mathbf{c}\rangle \\
=_{(b)} & \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{k}\in\mathbb{Z}^n} e^{-\pi\frac{\|\mathbf{x}\|^2(s^4+r^4)}{s^4r^2t^2}\left(\frac{M}{2}\mathbf{w}_{\mathbf{c},\mathbf{k}}\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\frac{M}{2}\mathbf{w}_{\mathbf{c},\mathbf{k}}\right)}\cdot e^{2\pi i\theta_{\mathbf{c},\mathbf{k}}}|\mathbf{c}\rangle\,,
\end{aligned}
\tag{54}
$$

where in (a) we use PSF from $\sum_{\mathbf{j}\in\mathbb{Z}^n}$ to $\sum_{\mathbf{k}\in\mathbb{Z}^n}$, and Eqn. (7); in (b) we use $M = 2(t^2+\|\mathbf{x}\|^2)$ (**C.2**) and drop in $R = s^2t^2$.

Note that

$$
\begin{aligned}
-\frac{M}{2}\mathbf{w}_{\mathbf{c},\mathbf{k}} = & \ \mathbf{c}+\mathbf{z}' - \mathbf{x}\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2} + \left(\mathbf{h}^* + \frac{\langle \mathbf{x},\mathbf{y}\rangle\,\mathbf{x}}{\|\mathbf{x}\|^2} - \mathbf{y}\right) - \frac{M}{2}\mathbf{k} \\
= & \ \mathbf{c}+\mathbf{z}'+\mathbf{h}^* - \mathbf{y} + \mathbf{x}\left(\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right) - \frac{M}{2}\mathbf{k}.
\end{aligned}
$$

To simplify the notations, recall in the statement of Lemma 3.27 where we denote

$$
\mathbf{c}' := \mathbf{c}+\mathbf{z}'+\mathbf{h}^* - \mathbf{y} + \mathbf{x}\left(\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2} - \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right). \tag{55}
$$

Therefore $\mathbf{c}+\mathbf{z}' - \frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x} = \mathbf{c}' - \left(\mathbf{h}^* - \mathbf{y} + \mathbf{x}\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)$.

Also recall from Condition **C.6** that we denote $\sigma = \frac{trs^2}{u\sqrt{s^4+r^4}}$. So we can rewrite $|\varphi_6\rangle$ in Eqn. (54) as

$$
|\varphi_6\rangle = \sum_{\mathbf{c}\in\mathbb{Z}_M^n}\sum_{\mathbf{k}\in\mathbb{Z}^n} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)}\cdot e^{2\pi i\mathbf{k}^T\cdot\frac{\mathbf{c}'-\left(\mathbf{h}^*-\mathbf{y}+\mathbf{x}\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)}{M}}\cdot e^{2\pi i\theta_{\mathbf{c}}}|\mathbf{c}\rangle\,, \tag{56}
$$

where $\theta_{\mathbf{c}} := -\frac{\left\|\mathbf{c}+\mathbf{z}'-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}\right\|^2}{M^2}$. Note that $e^{2\pi i\theta_{\mathbf{c}}}$ is a phase term that only depends on $\mathbf{c}$, not on $\mathbf{k}$.

Next, we reorganize the expression of $|\varphi_6\rangle$ in Eqn. (56) by splitting $\mathbf{k} \in \mathbb{Z}^n$ into $\mathbf{k_c}+\mathbf{k}$ where $\mathbf{k_c} \in 0|\mathbb{Z}^{n-1}$, $\mathbf{k} \in \mathbf{b}\mathbb{Z}$. Since the first coordinate of $\mathbf{b}$ is -1, there is a one-to-one mapping between $\mathbb{Z}^n$ and $0|\mathbb{Z}^{n-1} \times \mathbf{b}\mathbb{Z}$. Therefore $|\varphi_6\rangle$ can be equivalently written as

$$|\varphi_6\rangle = \sum_{\mathbf{c}\in\mathbb{Z}_M^n, \mathbf{k_c}\in 0|\mathbb{Z}^{n-1}} g\left(\mathbf{c}', \mathbf{k_c}\right) \cdot e^{2\pi i\theta_{\mathbf{c}}} |\mathbf{c}\rangle\,, \tag{57}$$

where $g(\mathbf{c}', \mathbf{k_c})$ is defined as

$$g(\mathbf{c}', \mathbf{k_c}) = \sum_{\mathbf{k}\in\frac{\mathbf{x}\mathbb{Z}}{D}} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c}'-\frac{M}{2}(\mathbf{k_c}+\mathbf{k})\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c}'-\frac{M}{2}(\mathbf{k_c}+\mathbf{k})\right)} \cdot e^{2\pi i(\mathbf{k_c}+\mathbf{k})^T\cdot\frac{\mathbf{c}'-\left(\mathbf{h}^*-\mathbf{y}+\mathbf{x}\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)}{M}}. \tag{58}$$

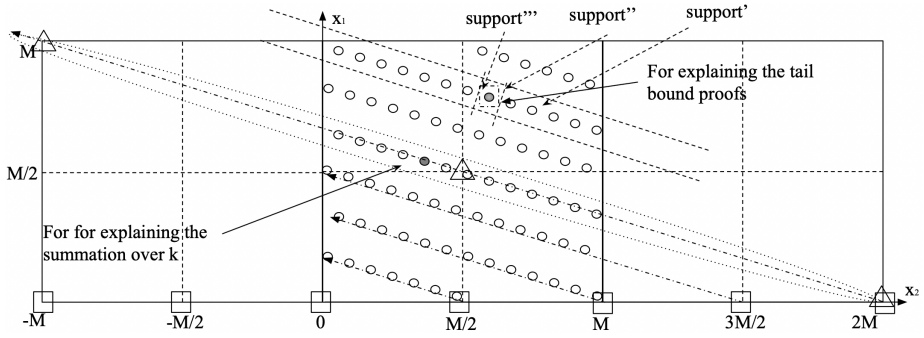

Figure 4: Explaining the support of $|\varphi_6\rangle$. In this example, $\mathbf{b} = (-1, 3)$.

As illustrated in Fig. 4, for the solid gray ball in the middle, the summation of $\mathbf{k} \in \mathbf{b}\mathbb{Z}$ in Eqn. (58) runs through the points in the triangles; the summation of $\mathbf{k_c} \in 0|\mathbb{Z}^{n-1}$ in Eqn. (57) runs through the points in the squares.

Next, for any $\mathbf{c}' - \frac{M}{2}\mathbf{k_c}$ in Eqn. (58), we write $\mathbf{c}' - \frac{M}{2}\mathbf{k_c} = \mathbf{c}_{\mathbf{x}}^{\perp} + \mathbf{c}_{\mathbf{x}}$, where

$$\mathbf{c}_{\mathbf{x}} := \mu\mathbf{x} := \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c}\right), \text{ and } \mathbf{c}_{\mathbf{x}}^{\perp} := \mathbf{c}' - \frac{M}{2}\mathbf{k_c} - \mathbf{c}_{\mathbf{x}} = \left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}' - \frac{M}{2}\mathbf{k_c}\right). \tag{59}$$

Therefore, $g(\mathbf{c}', \mathbf{k_c})$ in Eqn. (58) can be written as

$$\begin{aligned} g(\mathbf{c}', \mathbf{k_c}) = & \sum_{\mathbf{k}\in\frac{\mathbf{x}\mathbb{Z}}{D}} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c}_{\mathbf{x}}^{\perp}+\mathbf{c}_{\mathbf{x}}-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c}_{\mathbf{x}}^{\perp}+\mathbf{c}_{\mathbf{x}}-\frac{M}{2}\mathbf{k}\right)} \cdot e^{2\pi i(\mathbf{k_c}+\mathbf{k})^T\cdot\frac{\frac{M}{2}\mathbf{k_c}+\mathbf{c}_{\mathbf{x}}^{\perp}+\mathbf{c}_{\mathbf{x}}-\left(\mathbf{h}^*-\mathbf{y}+\mathbf{x}\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)}{M}} \\ =_{(a)} \; & e^{-\pi\frac{\|\mathbf{c}_{\mathbf{x}}^{\perp}\|^2}{\sigma^2}} e^{2\pi i\mathbf{k_c}^T\cdot\frac{\frac{M}{2}\mathbf{k_c}+\mathbf{c}_{\mathbf{x}}^{\perp}+\mathbf{c}_{\mathbf{x}}-\left(\mathbf{h}^*-\mathbf{y}+\mathbf{x}\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)}{M}} \\ & \cdot \underbrace{\sum_{\mathbf{k}\in\frac{\mathbf{x}\mathbb{Z}}{D}} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c}_{\mathbf{x}}-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c}_{\mathbf{x}}-\frac{M}{2}\mathbf{k}\right)} \cdot e^{2\pi i\mathbf{k}^T\cdot\frac{\frac{M}{2}\mathbf{k_c}+\mathbf{c}_{\mathbf{x}}-\mathbf{h}^*}{M}}}_{=:h(\mathbf{c}_{\mathbf{x}})}, \end{aligned} \tag{60}$$

where (a) holds since $\mathbf{k} \in \frac{\mathbf{x}\mathbb{Z}}{D}$, $\left\langle \mathbf{c}_{\mathbf{x}}^{\perp}, \mathbf{x} \right\rangle = 0$, $\mathbf{k}^T \cdot \frac{\mathbf{y} - \mathbf{x}\frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|^2}}{M} = 0$, and

$$\begin{aligned}
& \left(\mathbf{c}_{\mathbf{x}}^{\perp} + \mathbf{c}_{\mathbf{x}} - \frac{M}{2}\mathbf{k}\right)^T \cdot \left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R + T\|\mathbf{x}\|^2}\right) \cdot \left(\mathbf{c}_{\mathbf{x}}^{\perp} + \mathbf{c}_{\mathbf{x}} - \frac{M}{2}\mathbf{k}\right) \\
= & \left(\mathbf{c}_{\mathbf{x}}^{\perp T} + \left(\mathbf{c}_{\mathbf{x}} - \frac{M}{2}\mathbf{k}\right)^T \cdot \left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R + T\|\mathbf{x}\|^2}\right)\right) \cdot \left(\mathbf{c}_{\mathbf{x}}^{\perp} + \mathbf{c}_{\mathbf{x}} - \frac{M}{2}\mathbf{k}\right) \\
= & \|\mathbf{c}_{\mathbf{x}}^{\perp}\|^2 + \left(\mathbf{c}_{\mathbf{x}} - \frac{M}{2}\mathbf{k}\right)^T \cdot \left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R + T\|\mathbf{x}\|^2}\right) \cdot \left(\mathbf{c}_{\mathbf{x}} - \frac{M}{2}\mathbf{k}\right).
\end{aligned}$$

Let us continue expanding the $h(\mathbf{c}_{\mathbf{x}})$ term by writing it as a function of μ (recall that we define $\mu = \frac{\left\langle (\mathbf{c}' - \frac{M}{2}\mathbf{k}_{\mathbf{c}}), \mathbf{x} \right\rangle}{\|\mathbf{x}\|^2}$, $\mathbf{c}_{\mathbf{x}} = \mu\mathbf{x}$ in Eqn. (59)). Also, we replace $\mathbf{k} \in \frac{\mathbf{x}\mathbb{Z}}{D}$ by $\frac{\mathbf{x}k}{D}$ for $k \in \mathbb{Z}$. Then

$$\begin{aligned}
h(\mathbf{c}_{\mathbf{x}}) = & \sum_{k \in \mathbb{Z}} e^{-\pi \frac{1}{\sigma^2}\left(\mu\mathbf{x} - \frac{Mk}{2D}\mathbf{x}\right)^T \cdot \left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R + T\|\mathbf{x}\|^2}\right) \cdot \left(\mu\mathbf{x} - \frac{Mk}{2D}\mathbf{x}\right)} \cdot e^{2\pi i \frac{k}{D}\mathbf{x}^T \cdot \frac{\mu\mathbf{x} - (\mathbf{h}^* - \frac{M}{2}\mathbf{k}_{\mathbf{c}})}{M}} \\
= & \sum_{k \in \mathbb{Z}} e^{-\pi \frac{1}{\sigma^2}\left(\mu - \frac{Mk}{2D}\right) \cdot \mathbf{x}^T \left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R + T\|\mathbf{x}\|^2}\right)\mathbf{x} \cdot \left(\mu - \frac{Mk}{2D}\right)} \cdot e^{2\pi i \frac{k\left(\mu\|\mathbf{x}\|^2 - \left\langle \mathbf{h}^* - \frac{M}{2}\mathbf{k}_{\mathbf{c}}, \mathbf{x} \right\rangle\right)}{DM}} =: A(\mu)
\end{aligned} \tag{61}$$

It remains to analyze $A(\mu)$. Let us start from estimating $\mathbf{x}^T \left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R + T\|\mathbf{x}\|^2}\right)\mathbf{x} =: S + Ui$, where $S, U \in \mathbb{R}$ denote the real and imaginary parts. First,

$$\begin{aligned}
\frac{T}{R + T\|\mathbf{x}\|^2} = & \frac{s^2 - r^2 i}{s^2 t^2 + \|\mathbf{x}\|^2(s^2 - r^2 i)} = \frac{s^2 - r^2 i}{s^2(t^2 + \|\mathbf{x}\|^2) - \|\mathbf{x}\|^2 r^2 i} \\
= & \frac{(s^2 - r^2 i)(s^2(t^2 + \|\mathbf{x}\|^2) + \|\mathbf{x}\|^2 r^2 i)}{s^4(t^2 + \|\mathbf{x}\|^2)^2 + \|\mathbf{x}\|^4 r^4} \\
= & \frac{s^4(t^2 + \|\mathbf{x}\|^2) + \|\mathbf{x}\|^2 r^4 + (s^2\|\mathbf{x}\|^2 r^2 - s^2(t^2 + \|\mathbf{x}\|^2)r^2)i}{s^4(t^2 + \|\mathbf{x}\|^2)^2 + \|\mathbf{x}\|^4 r^4} \\
= & \frac{(s^4(t^2 + \|\mathbf{x}\|^2) + \|\mathbf{x}\|^2 r^4) - (s^2 t^2 r^2)i}{s^4(t^2 + \|\mathbf{x}\|^2)^2 + \|\mathbf{x}\|^4 r^4}.
\end{aligned}$$

To simplify the denominator of the expression above, we let

$$\epsilon := \frac{s^4(t^2 + \|\mathbf{x}\|^2)^2}{\|\mathbf{x}\|^4 r^4} \in O\left(\frac{\|\mathbf{x}\|^4 t^4 (t^2 + \|\mathbf{x}\|^2)^2}{\|\mathbf{x}\|^4 r^4}\right) \in O\left(\frac{M^4}{r^4}\right) \in_{\mathbf{C.8}} o(n^{-3}). \tag{62}$$

Then, the real part of $\mathbf{x}^T \left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R + T\|\mathbf{x}\|^2}\right)\mathbf{x}$ equals to

$$\begin{aligned}
S = & \|\mathbf{x}\|^2 - \frac{\|\mathbf{x}\|^4(s^4(t^2 + \|\mathbf{x}\|^2) + \|\mathbf{x}\|^2 r^4)}{s^4(t^2 + \|\mathbf{x}\|^2)^2 + \|\mathbf{x}\|^4 r^4} \\
= & \frac{s^4(t^2 + \|\mathbf{x}\|^2)^2\|\mathbf{x}\|^2 + \|\mathbf{x}\|^6 r^4 - \|\mathbf{x}\|^4 s^4(t^2 + \|\mathbf{x}\|^2) - \|\mathbf{x}\|^6 r^4}{s^4(t^2 + \|\mathbf{x}\|^2)^2 + \|\mathbf{x}\|^4 r^4} \\
= & \frac{s^4\|\mathbf{x}\|^2(t^4 + 2t^2\|\mathbf{x}\|^2 + \|\mathbf{x}\|^4 - t^2\|\mathbf{x}\|^2 - \|\mathbf{x}\|^4)}{s^4(t^2 + \|\mathbf{x}\|^2)^2 + \|\mathbf{x}\|^4 r^4} \\
= & \frac{s^4\|\mathbf{x}\|^2 t^2(t^2 + \|\mathbf{x}\|^2)}{s^4(t^2 + \|\mathbf{x}\|^2)^2 + \|\mathbf{x}\|^4 r^4} \in O\left(\left(\frac{s^2 t^2 \|\mathbf{x}\|}{r^2\|\mathbf{x}\|^2}\right)^2\right) \in_{\mathbf{C.5}} O\left(\left(\frac{t^4\|\mathbf{x}\|^3}{r^2\|\mathbf{x}\|^2}\right)^2\right) \in_{\mathbf{C.2}} O\left(\left(\frac{M^2\|\mathbf{x}\|}{r^2}\right)^2\right)
\end{aligned} \tag{63}$$

This means the width in the direction of $\mathbf{x}$ is in the order of $\frac{r^2}{M^2}$, which is larger than $M/2$. The imaginary part of $\mathbf{x}^T\left(\mathbf{I}_n - \frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\mathbf{x}$ is $U = \frac{s^2t^2r^2\|\mathbf{x}\|^4}{s^4(t^2+\|\mathbf{x}\|^2)^2+\|\mathbf{x}\|^4r^4}$. Note that $U > S$. We will use the following identity later in Eqn. (64):

$$\begin{aligned}
\frac{U}{\sigma^2}\cdot\left(\frac{M}{2D}\right)^2 &= \frac{\|\mathbf{x}\|^2(s^4+r^4)}{t^2r^2s^4}\frac{s^2t^2r^2\|\mathbf{x}\|^4}{s^4(t^2+\|\mathbf{x}\|^2)^2+\|\mathbf{x}\|^4r^4}\left(\frac{M}{2D}\right)^2 \\
&= \frac{\|\mathbf{x}\|^2(s^4+r^4)}{s^2}\frac{\|\mathbf{x}\|^4}{\|\mathbf{x}\|^4r^4}\cdot\frac{1}{1+\epsilon}\left(\frac{M}{2D}\right)^2 \\
&=_{\mathbf{C.5}} \frac{\|\mathbf{x}\|^2(s^4+r^4)}{r^4}\frac{r^4t^2}{2\|\mathbf{x}\|^2(s^4+r^4)(t^2+\|\mathbf{x}\|^2)^2}\left(\frac{M}{2D}\right)^2\frac{1}{1+\epsilon} \\
&=_{\mathbf{C.2}} \frac{t^2}{2D^2}\cdot(1+O(\epsilon))\,.
\end{aligned}$$

Given that $\frac{t^2}{2D^2}\in 2\mathbb{Z}$ (Condition **C.1**), we can write

$$\frac{U}{\sigma^2}\cdot\left(\frac{M}{2D}\right)^2 = \frac{t^2}{2D^2}(1+O(\epsilon)) = U'+U'',\ \text{where } U' := \frac{t^2}{2D^2}\in 2\mathbb{Z},\ U''\in O\left(\frac{t^2\epsilon}{D^2}\right). \tag{64}$$

Then $A(\mu)$ from Eqn. (61) equals to

$$\begin{aligned}
A(\mu) &= \sum_{k\in\mathbb{Z}} e^{-\pi\frac{S+Ui}{\sigma^2}\left(\mu-\frac{Mk}{2D}\right)^2}\cdot e^{2\pi i\frac{k\left(\mu\|\mathbf{x}\|^2-\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle\right)}{DM}} \\
&= \sum_{k\in\mathbb{Z}} e^{-\pi\left(\frac{S}{\sigma^2}+\frac{Ui}{\sigma^2}\right)\left(\frac{M}{2D}\right)^2\left(\frac{2D}{M}\mu-k\right)^2}\cdot e^{2\pi i\frac{k\left(\mu\|\mathbf{x}\|^2-\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle\right)}{DM}} \\
&=_{(a)} \sum_{k\in\mathbb{Z}} e^{-\pi\left(\frac{S}{\sigma^2}\left(\frac{M}{2D}\right)^2+U''i\right)\left(\frac{2D}{M}\mu-k\right)^2} e^{-\pi U'i\left(k^2-2\frac{2D}{M}\mu k+\left(\frac{2D}{M}\mu\right)^2\right)}\cdot e^{2\pi i\frac{k\left(\mu\|\mathbf{x}\|^2-\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle\right)}{DM}} \\
&=_{(b)} \sum_{k\in\mathbb{Z}} e^{-\pi\left(\frac{S}{\sigma^2}\left(\frac{M}{2D}\right)^2+U''i\right)\left(k-\frac{2D}{M}\mu\right)^2} e^{2\pi iU'\frac{2D}{M}\mu k} e^{-\pi iU'\left(\frac{2D}{M}\mu\right)^2}\cdot e^{2\pi i\frac{k\left(\mu\|\mathbf{x}\|^2-\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle\right)}{DM}} \\
&=_{(c)} \frac{1}{\sqrt{\frac{S}{\sigma^2}\left(\frac{M}{2D}\right)^2+U''i}}\cdot\sum_{j\in\mathbb{Z}} e^{-\pi\frac{1}{\frac{S}{\sigma^2}\left(\frac{M}{2D}\right)^2+U''i}\left(j-\frac{2D}{M}U'\mu-\frac{\mu\|\mathbf{x}\|^2-\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{DM}\right)^2}\cdot e^{2\pi i\theta(\mu,j)} \\
&=_{(d)} \frac{1}{\sqrt{\frac{S}{\sigma^2}\left(\frac{M}{2D}\right)^2+U''i}}\cdot\sum_{j\in\mathbb{Z}} e^{-\pi\frac{1}{\frac{S}{\sigma^2}\left(\frac{M}{2D}\right)^2+U''i}\left(j-\frac{1}{2D}\left(\mu-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)^2}\cdot e^{2\pi i\theta(\mu,j)}
\end{aligned} \tag{65}$$

where (a) uses Eqn. (64); (b) uses $U'\in 2\mathbb{Z}$; (c) uses PSF and keeps the phase term in $\theta(\mu,j)$; (d) uses

$$\begin{aligned}
\frac{2D}{M}U'\mu+\frac{\mu\|\mathbf{x}\|^2-\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{DM} &=_{U'=\frac{t^2}{2D^2}} \mu\frac{2D}{M}\frac{t^2}{2D^2}+\frac{\mu\|\mathbf{x}\|^2-\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{DM} \\
&= \mu\frac{t^2+\|\mathbf{x}\|^2}{DM}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{DM} = \frac{1}{2D}\left(\mu-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right).
\end{aligned} \tag{66}$$

So that $\theta(\mu, j)$ equals to

$$\begin{aligned}\theta(\mu,j) &:= -\frac{2D\mu}{M}\left(j-\frac{2D}{M}U'\mu-\frac{\mu\|\mathbf{x}\|^2-\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{DM}\right)-\frac{U'}{2}\left(\frac{2D}{M}\mu\right)^2\\ &=_{Eqn.(66),\ U'=\frac{t^2}{2D^2}} -\frac{2D\mu}{M}\left(j-\frac{1}{2D}\left(\mu-\frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)-\frac{t^2}{4D^2}\left(\frac{2D}{M}\mu\right)^2\\ &= -\frac{\mu}{M}\left(2Dj-\left(\mu-\frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)-\frac{t^2\mu^2}{M^2}.\end{aligned} \tag{67}$$

Note that in the direction parallel to $\mathbf{x}$,

$$\begin{aligned}&\mu-\frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}=\frac{\left\langle \mathbf{c}'-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\\ =\ &\frac{\langle \mathbf{c}',\mathbf{x}\rangle}{\|\mathbf{x}\|^2}-\frac{\langle \mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{t^2\left\langle \frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2(t^2+\|\mathbf{x}\|^2)}=\frac{\langle \mathbf{c},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}+\frac{t^2\left\langle \mathbf{z}'+\mathbf{h}^*,\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2(t^2+\|\mathbf{x}\|^2)}-\frac{t^2\langle \mathbf{k_c},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}.\end{aligned} \tag{68}$$

To put together the expression of $|\varphi_6\rangle$, recall from Eqn. (59) that $\mathbf{c_x}=\mu\mathbf{x}$, where $\mu=\frac{\left\langle \left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}$. Also recall from Eqn. (55) that $\mathbf{c}'=\mathbf{c}+\mathbf{z}'+\mathbf{h}^*-\mathbf{y}+\mathbf{x}\left(\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\right)$. We drop $A(\mu)$ (Eqn. (65)) into $h(\mathbf{c_x})$ (Eqn. (61)), then drop $h(\mathbf{c_x})$ in $g(\mathbf{c}',\mathbf{k_c})$ (Eqn. (58)), then drop $g(\mathbf{c}',\mathbf{k_c})$ in $|\varphi_6\rangle$ (Eqn. (57)), we get

$$\begin{aligned}|\varphi_6\rangle=\sum_{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1}} &e^{-\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right)\right\|^2}{\sigma^2}}e^{2\pi i\mathbf{k_c}^T\cdot\frac{\mathbf{c}+\mathbf{z}'-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}}{M}}\cdot e^{-2\pi i\frac{\left\|\mathbf{c}+\mathbf{z}'-\frac{\langle \mathbf{x},\mathbf{z}'\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}\right\|^2}{M^2}}\\ \cdot\sum_{j\in\mathbb{Z}}&e^{-\pi\frac{1}{W+U''i}\left(j-\frac{1}{2D}\left(\frac{\left\langle \left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)^2}\\ \cdot\ &e^{-2\pi i\left(\frac{\left\langle \left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{M\|\mathbf{x}\|^2}\left(2Dj-\left(\frac{\left\langle \left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)+\frac{t^2}{M^2}\frac{\left\langle \left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle^2}{\|\mathbf{x}\|^4}\right)}|\mathbf{c}\rangle\,,\end{aligned} \tag{69}$$

where

$$\begin{aligned}W:=\frac{S}{\sigma^2}\cdot\left(\frac{M}{2D}\right)^2 &=_{Eqn.\ (63)}\ \frac{s^4\|\mathbf{x}\|^2t^2(t^2+\|\mathbf{x}\|^2)}{r^4\|\mathbf{x}\|^4}\frac{1}{1+\epsilon}\frac{\|\mathbf{x}\|^2(s^4+r^4)}{t^2r^2s^4}\left(\frac{M}{2D}\right)^2\\ &=\ \frac{(t^2+\|\mathbf{x}\|^2)}{r^2}\frac{1+\frac{s^4}{r^4}}{1+\epsilon}\left(\frac{M}{2D}\right)^2=\frac{4(t^2+\|\mathbf{x}\|^2)^3}{r^2}\left(\frac{1}{2D}\right)^2\cdot\frac{1+\frac{s^4}{r^4}}{1+\epsilon}.\end{aligned} \tag{70}$$

Recall that $\sigma^2=\frac{t^2r^2s^4}{\|\mathbf{x}\|^2(s^4+r^4)}=_{\mathbf{C.5}}\frac{t^2r^2}{\|\mathbf{x}\|^2(s^4+r^4)}\cdot 4\frac{\|\mathbf{x}\|^4(s^4+r^4)^2}{r^8}\frac{(t^2+\|\mathbf{x}\|^2)^4}{t^4}=4\frac{\|\mathbf{x}\|^2(t^2+\|\mathbf{x}\|^2)^4}{r^2t^2}\cdot\left(1+\frac{s^4}{r^4}\right)$. So

$$W\cdot(2D\cdot\|\mathbf{x}\|)^2=\frac{4\|\mathbf{x}\|^2(t^2+\|\mathbf{x}\|^2)^3}{r^2}\cdot\frac{1+\frac{s^4}{r^4}}{1+\epsilon}=\sigma^2\cdot\frac{t^2}{t^2+\|\mathbf{x}\|^2}\cdot\frac{1}{1+\epsilon}\ \Rightarrow\ W\cdot(2D\cdot\|\mathbf{x}\|)^2\in(0.5,1)\cdot\sigma^2. \tag{71}$$

Also, $\frac{U''}{W}=_{(64),(70)}O\left(\frac{t^2\epsilon}{D^2}\cdot\frac{r^2D^2}{(t^2+\|\mathbf{x}\|^2)^3}\right)=_{(62)}O\left(\frac{t^2M^4}{r^4}\cdot\frac{r^2}{(t^2+\|\mathbf{x}\|^2)^3}\right)=O\left(\frac{M^2}{r^2}\right)\in_{\mathbf{C.8}}o(n^{-1})$. So $Re\left(\frac{1}{W+U''i}\right)=\frac{W}{W^2+U''^2}\in\frac{(2D)^2\|\mathbf{x}\|^2}{\sigma^2}\cdot(1,3)$. This concludes the proof of Lemma 3.27. □

Lemma 3.28. *The support of $|\varphi_6\rangle$ consists of $2^{n-1}\cdot\frac{M}{2D^2}$ elliptical Gaussian balls centered at $\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})-\mathbf{x}\langle\mathbf{x},\mathbf{k_c}\rangle+2Dj\mathbf{x}+\mathbf{x}\left(\frac{\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{\langle\mathbf{y},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)$, for some $\mathbf{k_c}\in 0|\mathbb{Z}^{n-1}$ and some $j\in\mathbb{Z}$.*

Proof. For those elliptical Gaussian balls, in the direction orthogonal to $\mathbf{x}$, the width is σ, the center is $\left(\mathbf{I}-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})\right)$; in the direction parallel to $\mathbf{x}$, the width is $\approx\sqrt{W}\cdot(2D\cdot\|\mathbf{x}\|)$, the center is $\left(2Dj-\frac{t^2\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{\|\mathbf{x}\|^2(t^2+\|\mathbf{x}\|^2)}+\frac{t^2\langle\mathbf{k_c},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)\mathbf{x}$ (following Eqn. (68)). Combining both directions, the centers are

$$\begin{aligned}
&\left(\mathbf{I}-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})\right)+\left(2Dj-\frac{t^2\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{\|\mathbf{x}\|^2(t^2+\|\mathbf{x}\|^2)}+\frac{t^2\langle\mathbf{k_c},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)\mathbf{x}\\
=\;&\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\left(\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})\right)+\left(2Dj-\frac{t^2\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{\|\mathbf{x}\|^2(t^2+\|\mathbf{x}\|^2)}+\frac{t^2\langle\mathbf{k_c},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)\mathbf{x} \qquad (72)\\
=\;&\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})-\mathbf{x}\langle\mathbf{x},\mathbf{k_c}\rangle+2Dj\mathbf{x}+\mathbf{x}\left(\frac{\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{\langle\mathbf{y},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right),
\end{aligned}$$

for some $\mathbf{k_c}\in 0|\mathbb{Z}^{n-1}$ and some $j\in\mathbb{Z}$. □

Next we prove the tail bounds of the Gaussian balls in the support of $|\varphi_6\rangle$. For W,U'' defined in Eqns. (70), (64). For $\mathbf{c}\in\mathbb{Z}_M^n$, $\mathbf{k_c}\in 0|\mathbb{Z}^{n-1}$, $j\in\mathbb{Z}$, recall that $\mathbf{c'}=\mathbf{c}+\mathbf{z'}+\mathbf{h}^*-\mathbf{y}+\mathbf{x}\left(\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}-\frac{\langle\mathbf{x},\mathbf{z'}\rangle}{t^2+\|\mathbf{x}\|^2}\right)$ is defined in Eqn. (55). Let

$$g_6(\mathbf{c},\mathbf{k_c},j):=e^{-\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right)\right\|^2}{\sigma^2}}\cdot e^{-\pi\frac{W}{W^2+U''^2}\left(j-\frac{1}{2D}\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)^2}\cdot e^{2\pi i\phi_6(\mathbf{c},\mathbf{k_c},j)}, \qquad (73)$$

where $e^{2\pi i\phi_6'(\mathbf{c},\mathbf{k_c},j)}$ contains the phase terms and the imaginary part of $e^{-\pi\frac{-U''i}{W^2+U''^2}\cdots}$, i.e.,

$$\begin{aligned}
e^{2\pi i\phi_6'(\mathbf{c},\mathbf{k_c},j)}:=\;&e^{2\pi i\mathbf{k_c}^T\cdot\frac{\mathbf{c}+\mathbf{z'}-\frac{\langle\mathbf{x},\mathbf{z'}\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}}{M}}\cdot e^{-2\pi i\frac{\left\|\mathbf{c}+\mathbf{z'}-\frac{\langle\mathbf{x},\mathbf{z'}\rangle}{t^2+\|\mathbf{x}\|^2}\mathbf{x}\right\|^2}{M^2}}e^{-\pi\frac{-U''i}{W^2+U''^2}\left(j-\frac{1}{2D}\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)^2}\\
&\cdot e^{-2\pi i\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{M\|\mathbf{x}\|^2}\left(2Dj-\left(\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)+\frac{t^2}{M^2}\frac{\left\langle\left(\mathbf{c'}-\frac{M}{2}\mathbf{k_c}\right),\mathbf{x}\right\rangle^2}{\|\mathbf{x}\|^4}\right)}.
\end{aligned}$$

Then $|\varphi_6\rangle=\sum_{\mathbf{c}\in\mathbb{Z}_M^n,\mathbf{k_c}\in 0|\mathbb{Z}^{n-1},j\in\mathbb{Z}}g_6(\mathbf{c},\mathbf{k_c},j)\,|\mathbf{c}\rangle$.

In Lemma 3.29 we show that $|\varphi_6\rangle\approx_t|\varphi_6'\rangle\approx_t|\varphi_6''\rangle\approx_t|\varphi_6'''\rangle$ (our goal is to show $|\varphi_6\rangle\approx_t|\varphi_6'''\rangle$, but we introduce two intermediate steps for clarity), where $|\varphi_6'\rangle$, $|\varphi_6''\rangle$, $|\varphi_6'''\rangle$ are defined as follows:

$$|\varphi_6'\rangle:=\sum_{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1},\ j\in\mathbb{Z}\text{ s.t. }\operatorname{dist}(\mathbf{c'}-\frac{M}{2}\mathbf{k_c},\mathbf{x}\mathbb{R})\le\sigma\sqrt{n}\log n}g_6(\mathbf{c},\mathbf{k_c},j)\,|\mathbf{c}\rangle, \qquad (74)$$

$$|\varphi_6''\rangle:=\sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1},\ j\in\mathbb{Z}\text{ s.t. }\operatorname{dist}(\mathbf{c'}-\frac{M}{2}\mathbf{k_c},\mathbf{x}\mathbb{R})\le\sigma\sqrt{n}\log n\\ \text{and }\left|\frac{\left\langle\mathbf{c'}-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{\|\mathbf{x}\|^2}-\frac{\left\langle\mathbf{h}^*-\frac{M}{2}\mathbf{k_c},\mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}-2Dj\right|\le\frac{\sigma\sqrt{n}\log n}{\|\mathbf{x}\|}}}g_6(\mathbf{c},\mathbf{k_c},j)\,|\mathbf{c}\rangle, \qquad (75)$$

$$\left|\varphi_6'''\right\rangle := \sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1},\ j\in\mathbb{Z}\text{ s.t.}\\ \left\|\frac{M}{2}\mathbf{k_c}-(\mathbf{z'}+\mathbf{h}^*-\mathbf{y})-\mathbf{x}\langle\mathbf{x},\mathbf{k_c}\rangle+2Dj\mathbf{x}+\mathbf{x}\left(\frac{\langle\mathbf{z'}+\mathbf{h}^*,\mathbf{x}\rangle}{t^2+\|\mathbf{x}\|^2}-\frac{\langle\mathbf{y},\mathbf{x}\rangle}{\|\mathbf{x}\|^2}\right)-\mathbf{c}\right\|_\infty\leq\sigma\log n}} g_6(\mathbf{c},\mathbf{k_c},j)\left|\mathbf{c}\right\rangle, \tag{76}$$

As illustrated in Fig. 4, for the gradient gray ball on the top, the support of $\left|\varphi_6'\right\rangle$ is *support*′ (between two dashed lines parallel to $\mathbf{x}$), the support of $\left|\varphi_6''\right\rangle$ is *support*″, the support of $\left|\varphi_6'''\right\rangle$ is *support*‴.

Lemma 3.29. $\left|\varphi_6\right\rangle \approx_t \left|\varphi_6'\right\rangle \approx_t \left|\varphi_6''\right\rangle \approx_t \left|\varphi_6'''\right\rangle$.

Proof. We treat $\left|\varphi_6\right\rangle, \left|\varphi_6'\right\rangle, \left|\varphi_6''\right\rangle, \left|\varphi_6'''\right\rangle$ as unnormalized vectors. Between $\left|\varphi_6\right\rangle, \left|\varphi_6'\right\rangle$, it is in fact easier to use the expression of $\left|\varphi_6\right\rangle$ from Eqn. (56) and the equal expression of $\left|\varphi_6'\right\rangle$ as follows:

$$\left|\varphi_6'\right\rangle = \sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k}\in\mathbb{Z}^n,\\ \mathrm{dist}(\mathbf{c'}-\frac{M}{2}\mathbf{k},\mathbf{x}\mathbb{R})\leq\sigma\sqrt{n}\log n}} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)}\cdot e^{2\pi i\mathbf{k}^T\cdot\frac{\mathbf{c'}-\left(\mathbf{h}^*-\mathbf{y}+\mathbf{x}\frac{\langle\mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\right)}{M}}\cdot e^{2\pi i\theta_{\mathbf{c}}}\left|\mathbf{c}\right\rangle. \tag{77}$$

Note that the expressions of $\left|\varphi_6'\right\rangle$ in Eqn. (77) and Eqn. (75) only differ by a normalization factor of $\frac{1}{\sqrt{W+U''i}}$ appeared in Eqn. (65), and we can verify that $\frac{1}{|\sqrt{W+U''i}|}\in\left(\frac{1}{\mathrm{poly}(n)},\mathrm{poly}(n)\right)$.

Then we have

$$\begin{aligned}
&\left\||\varphi_6\rangle-\left|\varphi_6'\right\rangle\right\|_1\\
\leq&\sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k}\in\mathbb{Z}^n,\\ \mathrm{dist}(\mathbf{c'}-\frac{M}{2}\mathbf{k},\mathbf{x}\mathbb{R})>\sigma\sqrt{n}\log n}} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)}\\
=_{(a)}&\sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\mathbf{k}\in\mathbb{Z}^n,\delta\in\frac{\mathbb{Z}}{t^2+\|\mathbf{x}\|^2},\left\langle\mathbf{c'}-\frac{M}{2}\mathbf{k},\mathbf{x}\right\rangle=\delta\\ \mathrm{dist}(\mathbf{c'}-\frac{M}{2}\mathbf{k},\mathbf{x}\mathbb{R})>\sigma\sqrt{n}\log n}} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)}\cdot e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\frac{R\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2(R+T\|\mathbf{x}\|^2)}\right)\cdot\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)}\\
\leq_{(b)}&\sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\mathbf{k}\in\mathbb{Z}^n,\delta\in\frac{\mathbb{Z}}{t^2+\|\mathbf{x}\|^2},\left\langle\mathbf{c'}-\frac{M}{2}\mathbf{k},\mathbf{x}\right\rangle=\delta\\ \mathrm{dist}(\mathbf{c'}-\frac{M}{2}\mathbf{k},\mathbf{x}\mathbb{R})>\sigma\sqrt{n}\log n}} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c'}-\frac{M}{2}\mathbf{k}\right)}\cdot e^{-\pi\frac{\delta^2}{\sigma^2\cdot(10r^2\|\mathbf{x}\|^2)^2}}\\
\leq_{(c)}&\sum_{\mathbf{c}\in\mathbb{Z}_M^n} e^{-\pi n\log^2 n}\cdot\rho_\sigma\left(\frac{M}{2}L_{assist}\right)\cdot\sum_{\delta\in\frac{\mathbb{Z}}{t^2+\|\mathbf{x}\|^2}} e^{-\pi\frac{\delta^2}{\sigma^2\cdot(10r^2\|\mathbf{x}\|^2)^2}}\\
\leq_{(d)}&M^n\cdot e^{-\pi n\log^2 n}\cdot\rho_\sigma\left(\frac{M}{2}\mathbb{Z}^n\right)\cdot\mathrm{poly}(n)\leq_{(e)} e^{-\pi n\log^2 n}\cdot\mathrm{poly}(n)\in 2^{-\Omega(n)},
\end{aligned} \tag{78}$$

where in (a) we use $\mathbf{I}_n-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}=\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}+\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}-\frac{T\mathbf{x}\mathbf{x}^T}{R+T\|\mathbf{x}\|^2}=\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}+\frac{R\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2(R+T\|\mathbf{x}\|^2)}$, and we also fix $\left\langle\mathbf{c'}-\frac{M}{2}\mathbf{k},\mathbf{x}\right\rangle$ to be δ for $\delta\in\frac{\mathbb{Z}}{t^2+\|\mathbf{x}\|^2}$; in (b) we use

$$Re\left(\frac{R}{\|\mathbf{x}\|^2(R+T\|\mathbf{x}\|^2)}\right)=Re\left(\frac{s^2t^2}{\|\mathbf{x}\|^2(s^2t^2+s^2\|\mathbf{x}\|^2-r^2\|\mathbf{x}\|^2i)}\right)\geq\frac{1}{(10r^2\|\mathbf{x}\|^2)^2};$$

in (c) we use an assistant lattice $L_{assist} := \{\mathbf{k} \mid \mathbf{k} \in \mathbb{Z}^n, \langle \mathbf{k}, \mathbf{x} \rangle = 0\} \subset \mathbb{Z}^n$, and for all $\delta \in \frac{\mathbb{Z}}{t^2+\|\mathbf{x}\|^2}$, for all $\mathbf{c} \in \mathbb{Z}_M^n$, let $L_{assist} + \mathbf{d}$ be the coset of L_{assist} such that for $\mathbf{k} \in L_{assist} + \mathbf{d}$, $\left\langle \mathbf{c}' - \frac{M}{2}\mathbf{k}, \mathbf{x} \right\rangle = \delta$, then

$$\begin{aligned}
& \sum_{\mathbf{k}\in\mathbb{Z}^n, \left\langle \mathbf{c}'-\frac{M}{2}\mathbf{k}, \mathbf{x}\right\rangle = \delta, \mathrm{dist}(\mathbf{c}'-\frac{M}{2}\mathbf{k}, \mathbf{x}\mathbb{R}) > \sigma\sqrt{n}\log n} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)} \\
= & \sum_{\mathbf{k}\in L_{assist}+\mathbf{d}, \mathrm{dist}(\mathbf{c}'-\frac{M}{2}\mathbf{k}, \mathbf{x}\mathbb{R}) > \sigma\sqrt{n}\log n} e^{-\pi\frac{1}{\sigma^2}\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)^T\cdot\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\cdot\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)} \\
= & \sum_{\mathbf{k}\in L_{assist}+\mathbf{d}, \left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)\right\| > \sigma\sqrt{n}\log n} e^{-\pi\frac{1}{\sigma^2}\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}'-\frac{M}{2}\mathbf{k}\right)\right\|^2} \\
=_{(*)} & \sum_{\mathbf{k}'\in L_{assist}+\mathbf{n}, \left\|\frac{M}{2}\mathbf{k}'\right\| > \sigma\sqrt{n}\log n} e^{-\pi\frac{1}{\sigma^2}\left\|\frac{M}{2}\mathbf{k}'\right\|^2} \leq_{(**)} e^{-\pi n\log^2 n}\cdot\rho_\sigma\left(\frac{M}{2}L_{assist}\right),
\end{aligned}$$

where $(*)$ uses $\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}' - \frac{M}{2}\mathbf{k}\right) = \left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\mathbf{c}' - \frac{M}{2}\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\mathbf{k}$, and $\left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\mathbf{k} \in L_{assist} + \left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\mathbf{d}$, so we define $\mathbf{n} := \left(\mathbf{I}_n - \frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}' - \frac{M}{2}\mathbf{d}\right)$, then $(*)$ holds; $(**)$ follows from Lemma 2.5. In Item (d) of Eqn. (78) we use $\rho_\sigma\left(\frac{M}{2}L_{assist}\right) \leq \rho_\sigma\left(\frac{M}{2}\mathbb{Z}^n\right)$, and $t^2 + \|\mathbf{x}\|^2, \sigma\cdot(10r^2\|\mathbf{x}\|^2) \in \mathrm{poly}(n)$ so that $\sum_{\delta\in\frac{\mathbb{Z}}{t^2+\|\mathbf{x}\|^2}} e^{-\pi\frac{\delta^2}{\sigma^2\cdot(10r^2\|\mathbf{x}\|^2)^2}} \in \mathrm{poly}(n)$; in (e) we use $M, \sigma \in \mathrm{poly}(n)$, and Lemma 2.7.

Between $|\varphi_6'\rangle$ in Eqn. (74) and $|\varphi_6''\rangle$ in Eqn. (75), we have

$$\begin{aligned}
\left\| |\varphi_6'\rangle - |\varphi_6''\rangle \right\|_1 \leq & \sum_{\substack{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1},\ j\in\mathbb{Z}\text{ s.t. }\mathrm{dist}(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}, \mathbf{x}\mathbb{R})\leq\sigma\sqrt{n}\log n \\ \text{and }\left|\frac{\left\langle \mathbf{c}'-\frac{M}{2}\mathbf{k_c}, \mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c}, \mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2} - 2Dj\right| > \frac{\sigma\sqrt{n}\log n}{\|\mathbf{x}\|}}} e^{-\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right)\right\|^2}{\sigma^2}} \\
& \cdot e^{-\pi\frac{W}{W^2+U''^2}\left(j-\frac{1}{2D}\left(\frac{\left\langle\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right), \mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c}, \mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2}\right)\right)^2} \\
\leq_{(a)} & \sum_{\mathbf{c}\in\mathbb{Z}_M^n,\ \mathbf{k_c}\in 0|\mathbb{Z}^{n-1}\text{ s.t. }\mathrm{dist}(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}, \mathbf{x}\mathbb{R})\leq\sigma\sqrt{n}\log n} \rho_W(\mathbb{Z})\cdot 2^{-\Omega(n\log^2 n)} \\
\leq_{(b)} & M^n\cdot\rho_W(\mathbb{Z})\cdot 2^{-\Omega(n\log^2 n)} \in_{(c)} 2^{-\Omega(n\log^2 n)},
\end{aligned}$$

where in (a) we fix $\mathbf{c}, \mathbf{k_c}$, and apply Lemma 2.5 with $\left|\frac{\left\langle \mathbf{c}'-\frac{M}{2}\mathbf{k_c}, \mathbf{x}\right\rangle}{\|\mathbf{x}\|^2} - \frac{\left\langle \mathbf{h}^*-\frac{M}{2}\mathbf{k_c}, \mathbf{x}\right\rangle}{t^2+\|\mathbf{x}\|^2} - 2Dj\right| > \frac{\sigma\sqrt{n}\log n}{\|\mathbf{x}\|}$ over $j \in \mathbb{Z}$; in (a) we also use $e^{-\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\left(\mathbf{c}'-\frac{M}{2}\mathbf{k_c}\right)\right\|^2}{\sigma^2}} \leq 1$; in (b) we use the fact that for each $\mathbf{c} \in \mathbb{Z}_M^n$, there is at most $\left\lceil\frac{\sigma\sqrt{n}\log n}{M}\right\rceil \leq 1$ vector $\mathbf{k_c} \in 0|\mathbb{Z}^{n-1}$ such that $\mathrm{dist}(\mathbf{c}' - \frac{M}{2}\mathbf{k_c}, \mathbf{x}\mathbb{R}) \leq \sigma\sqrt{n}\log n$; in (c) we use $M \in \mathrm{poly}(n)$, and also $W \in \mathrm{poly}(n)$ (derived from Eqn. (71)) and Lemma 2.7 to conclude that $\rho_W(\mathbb{Z}) \in \mathrm{poly}(n)$.

To get a lower bound for $\| |\varphi_6''\rangle \|_2^2$, recall from Lemma 3.28 that the support consists of $2^{n-1}\cdot\frac{M}{2D^2}$ elliptical

Gaussian balls, so

$$\left\||\varphi_6''\rangle\right\|_2^2 \geq 2^{n-1}\cdot\frac{M}{2D^2}\cdot\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})\cap\sigma\sqrt{n}\mathcal{B}_2^n} e^{-2\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}}\cdot e^{-2\pi\frac{(\langle\mathbf{d},\mathbf{x}\rangle)^2}{\|\mathbf{x}\|^2\sigma_x^2}},$$

for some vector $\mathbf{u}\in[-0.5,0.5)^n$ which takes care of the fact that the centers of the elliptical Gaussian balls are not necessarily in $\mathbb{Z}^n$; σ_x satisfies $\sigma_x\in(0.3,1)\sigma$, so $\frac{\sigma^2-\sigma_x^2}{\sigma_x^2}\in(0,11)$. Note that

$$\begin{aligned}
&\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})\cap\sigma\sqrt{n}\mathcal{B}_2^n} e^{-2\pi\frac{\left\|\left(\mathbf{I}_n-\frac{\mathbf{x}\mathbf{x}^T}{\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}}\cdot e^{-2\pi\frac{(\langle\mathbf{d},\mathbf{x}\rangle)^2}{\|\mathbf{x}\|^2\sigma_x^2}}\\
=&\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})\cap\sigma\sqrt{n}\mathcal{B}_2^n} e^{-2\pi\frac{\left\|\left(\mathbf{I}_n+\frac{(\sigma^2-\sigma_x^2)\mathbf{x}\mathbf{x}^T}{\sigma_x^2\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}} \qquad (79)\\
=&\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})} e^{-2\pi\frac{\left\|\left(\mathbf{I}_n+\frac{(\sigma^2-\sigma_x^2)\mathbf{x}\mathbf{x}^T}{\sigma_x^2\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}}-\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})\setminus\sigma\sqrt{n}\mathcal{B}_2^n} e^{-2\pi\frac{\left\|\left(\mathbf{I}_n+\frac{(\sigma^2-\sigma_x^2)\mathbf{x}\mathbf{x}^T}{\sigma_x^2\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}}\\
\geq_{(a)}&\ \frac{1}{12}\left(\frac{\sigma}{\sqrt{2}}\right)^n(1-\mathrm{negl}(n))-2^{-\Omega(n)}\cdot\left(\frac{\sigma}{\sqrt{2}}\right)^n\in\frac{1}{12}\left(\frac{\sigma}{\sqrt{2}}\right)^n\cdot(1-\mathrm{negl}(n))
\end{aligned}$$

where (a) is obtained as follows: let $\mathbf{B}_a:=\left(\mathbf{I}_n+\frac{(\sigma^2-\sigma_x^2)\mathbf{x}\mathbf{x}^T}{\sigma_x^2\|\mathbf{x}\|^2}\right)$ be the basis of an assistant lattice L_a. Then $\det(L_a)=1+\frac{(\sigma^2-\sigma_x^2)}{\sigma_x^2}\in(1,12)$, $\lambda_n(L_a)\leq 12$, and $\lambda_1(L_a^*)\geq\frac{1}{12}$. Let $\mathbf{u}':=\mathbf{B}_a\mathbf{u}$. Then

$$\begin{aligned}
\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})} e^{-2\pi\frac{\left\|\left(\mathbf{I}_n+\frac{(\sigma^2-\sigma_x^2)\mathbf{x}\mathbf{x}^T}{\sigma_x^2\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}}=\rho_{\frac{\sigma}{\sqrt{2}}}(L_a+\mathbf{u}')=_{(b)}&\ \frac{1}{\det(L_a)}\left(\frac{\sigma}{\sqrt{2}}\right)^n\sum_{\mathbf{w}\in L_a^*}\rho_{\frac{\sqrt{2}}{\sigma}}(\mathbf{w})\cdot e^{2\pi i\langle\mathbf{w},\mathbf{u}'\rangle}\\
\geq_{(c)}&\ \frac{1}{12}\left(\frac{\sigma}{\sqrt{2}}\right)^n(1-\mathrm{negl}(n)),
\end{aligned}$$

where (b) uses PSF and Eqn. (4); (c) uses $\sigma>2\log n$, $\det(L_a)\leq 12$, $\lambda_1(L_a^*)\geq\frac{1}{12}$ and Lemma 2.6. And

$$\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})\setminus\sigma\sqrt{n}\mathcal{B}_2^n} e^{-2\pi\frac{\left\|\left(\mathbf{I}_n+\frac{(\sigma^2-\sigma_x^2)\mathbf{x}\mathbf{x}^T}{\sigma_x^2\|\mathbf{x}\|^2}\right)\mathbf{d}\right\|^2}{\sigma^2}}\leq\sum_{\mathbf{d}\in(\mathbb{Z}^n+\mathbf{u})\setminus\sigma\sqrt{n}\mathcal{B}_2^n} e^{-2\pi\frac{\|\mathbf{d}\|^2}{\sigma^2}}\leq 2^{-\Omega(n)}\cdot\rho_{\frac{\sigma}{\sqrt{2}}}(\mathbb{Z}^n)\in_{Lemma\ 2.7}2^{-\Omega(n)}\cdot\left(\frac{\sigma}{\sqrt{2}}\right)^n.$$

Hence Item (a) in Eqn (79) holds.

So $\left\||\varphi_6''\rangle\right\|_2^2\geq 2^{n-1}\cdot\frac{M}{2D^2}\cdot\frac{1}{12}\left(\frac{\sigma}{\sqrt{2}}\right)^n\cdot(1\pm\mathrm{negl}(n))$. Therefore,

$$\left\||\varphi_6''\rangle-|\varphi_6'\rangle\right\|_2\leq\left\||\varphi_6''\rangle-|\varphi_6'\rangle\right\|_1\in 2^{-\Omega(n\log^2 n)}\left\||\varphi_6''\rangle\right\|_2. \qquad (80)$$

Between $|\varphi_6''\rangle$ and $|\varphi_6'''\rangle$, we use the fact that the Gaussian balls in $|\varphi_6''\rangle$ are separated: in the direction parallel to $\mathbf{x}$, the gap is $2D\|\mathbf{x}\|>_{\mathbf{C.8}}2\sigma\sqrt{n}\log n$; in the direction orthogonal to $\mathbf{x}$, the gap is at least

$\frac{M}{2\|\mathbf{b}\|} >_{\mathbf{C.8}} 2\sigma\sqrt{n}\log n$. Therefore,

$$\left\| |\varphi_6''\rangle - |\varphi_6'''\rangle \right\|_2^2 \leq_{Lemma\ 2.6} 2^{n-1} \cdot \frac{M}{2D^2} \cdot \mathrm{negl}(n) \cdot \rho_{\frac{\sigma}{\sqrt{2}}}(\mathbb{Z}^n) \leq \mathrm{negl}(n) \cdot \left\| |\varphi_6''\rangle \right\|_2^2 .$$

From Eqn (80), we can also derive that $\left\| |\varphi_6'\rangle \right\|_2 \in (1 \pm \mathrm{negl}(n)) \left\| |\varphi_6''\rangle \right\|_2$. So

$$\left\| |\varphi_6\rangle - |\varphi_6'\rangle \right\|_2 \leq \left\| |\varphi_6\rangle - |\varphi_6'\rangle \right\|_1 \in \mathrm{negl}(n) \cdot \left\| |\varphi_6'\rangle \right\|_2 .$$

Then $|\varphi_6\rangle \approx_t |\varphi_6'\rangle \approx_t |\varphi_6''\rangle \approx_t |\varphi_6'''\rangle$ follows Lemma 2.11. □

3.7 Additional discussions

3.7.1 Additional observations from Step 2

The state obtained in Step 2 is not completely random (see Figure 2 (b)). The feature of Karst wave could have already appeared here. There was even an opportunity of solving LWE directly in Step 2, but our attempt wasn't successful. However, the feature we observe in Step 2 motivates us to split the modulus in Step 3 to 5, so let us explain the observations here.

Recall from Eqn. (18) that the expression of $|\varphi_2\rangle$ satisfies

$$|\varphi_2\rangle \approx_t \sum_{\mathbf{z}\in\mathbb{Z}_P^n} \sum_{j\in\mathbb{Z}} \exp\left(-\pi \frac{s^2 r^2 (s^2 - r^2 i)}{\|\mathbf{x}\|^2 (s^4 + r^4)} \left(j + \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P} \right)^2 \right) e^{-2\pi i \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\left(j + \frac{\langle \mathbf{x},\mathbf{z}\rangle}{P}\right)} e^{2\pi i \langle \mathbf{y}, \frac{\mathbf{z}}{P}\rangle} |\mathbf{z}\rangle .$$

Suppose $\frac{s^2 r^4}{\|\mathbf{x}\|^2(s^4+r^4)} = 2\nu$ for some $\nu \in \mathbb{Z}$ (this is not necessarily consistent with Cond. **C.5**, but Cond. **C.5** is never used before Step 2, so let us just assume $\frac{s^2 r^4}{\|\mathbf{x}\|^2(s^4+r^4)} \in 2\mathbb{Z}$ for now), then for $j \in \mathbb{Z}$,

$$\exp\left(\pi i \frac{s^2 r^4}{\|\mathbf{x}\|^2 (s^4 + r^4)} \left(j + \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P} \right)^2 \right) = \exp\left(2\pi i \nu \left(2j \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P} + \frac{\langle \mathbf{x}, \mathbf{z}\rangle^2}{P^2} \right) \right) = e^{2\pi i \nu 2j \frac{\langle \mathbf{x},\mathbf{z}\rangle}{P}} e^{2\pi i \nu \frac{\langle \mathbf{x},\mathbf{z}\rangle^2}{P^2}} .$$

This means

$$\begin{aligned} |\varphi_2\rangle &\approx_t \sum_{\mathbf{z}\in\mathbb{Z}_P^n} \sum_{j\in\mathbb{Z}} \exp\left(-\pi \frac{s^4 r^2}{\|\mathbf{x}\|^2 (s^4 + r^4)} \left(j + \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P} \right)^2 \right) e^{2\pi i \nu 2j \frac{\langle \mathbf{x},\mathbf{z}\rangle}{P}} e^{2\pi i \nu \frac{\langle \mathbf{x},\mathbf{z}\rangle^2}{P^2}} e^{-2\pi i \frac{\langle \mathbf{x},\mathbf{y}\rangle}{\|\mathbf{x}\|^2}\left(j + \frac{\langle \mathbf{x},\mathbf{z}\rangle}{P}\right)} e^{2\pi i \langle \mathbf{y}, \frac{\mathbf{z}}{P}\rangle} |\mathbf{z}\rangle \\ &=_{PSF} \sum_{\mathbf{z}\in\mathbb{Z}_P^n} \sum_{k\in\mathbb{Z}} \exp\left(-\pi \frac{\|\mathbf{x}\|^2 (s^4 + r^4)}{s^4 r^2} \left(k + \frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{x}\|^2} - 2\nu \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P} \right)^2 \right) e^{2\pi i \phi(k,\mathbf{z})} |\mathbf{z}\rangle , \end{aligned}$$

where $\phi(k, \mathbf{z})$ includes all phase terms.

Suppose we measure $\mathbf{z}$ now, we get some $\mathbf{z} \in \mathbb{Z}_P^n$ such that

$$\frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{x}\|^2} - 2\nu \frac{\langle \mathbf{x}, \mathbf{z}\rangle}{P} \in \mathbb{Z} + e, \text{ where } |e| \leq \frac{s^2}{\|\mathbf{x}\| r} \log n \approx \frac{2\nu \|\mathbf{x}\|}{r} \log n. \tag{81}$$

If we multiply both sides of Eqn. (81) by $\frac{P}{2\nu}$, we get

$$\frac{P\langle \mathbf{x}, \mathbf{y}\rangle}{2\nu\|\mathbf{x}\|^2} - \langle \mathbf{x}, \mathbf{z}\rangle \in P\mathbb{Z} + e', \text{ where } |e'| \leq \frac{P\|\mathbf{x}\|}{r}\log n. \tag{82}$$

Although we don't know the vector $\mathbf{y}$, we can set parameters P, ν so that $\frac{P}{2\nu\|\mathbf{x}\|^2} \in N\mathbb{Z}$ for some integer $N \geq 2$ and $\frac{P}{N} \in \mathbb{Z}$, which means $\frac{P\langle \mathbf{x},\mathbf{y}\rangle}{2\nu\|\mathbf{x}\|^2} \in N\mathbb{Z}$. Then we get $\langle \mathbf{x}, \mathbf{z}\rangle \equiv e' \pmod N$. If we can make sure $e' = 0$ with probability more than $1 - \frac{1}{n}$, then we can run Steps 1 to 2 for $O(n)$ times and get $O(n)$ many vectors $\{\mathbf{z}_i\}_{i\in O(n)}$ and solve $\mathbf{x}$ by solving modular linear equations with coefficients $\{\mathbf{z}_i\}_{i\in O(n)}$. However, we can only guarantee $|e'| \leq \frac{P\|\mathbf{x}\|}{r}\log n$, where $\frac{P}{r}$ is inherently greater than 1. So the idea above does not work.

The observation in Step 2 motivates us to work on a smaller modulus – imagine if we don't need to multiply both sides of Eqn. (81) by $\frac{P}{2\nu}$, but by a smaller factor, then the error term e' may not be that large. With the motivation of reducing the modulus, we come up with the idea of modulus splitting, as is done in Steps 3 to 5.

Acknowledgment

I would like to sincerely thank Andrew Yao for his tremendous support, encouragement, and frequent, insightful discussions about this project. I would like to thank Oded Regev for recommending the paper of Yi-Kai Liu [Liu09] to me in 2020, and giving me valuable suggestions on an earlier version of this manuscript. I would also like to thank Zihan Hu, Qipeng Liu, Han Luo, and Yaxin Tu for discussing other attempts of designing quantum algorithms for solving LWE, and giving me valuable suggestions on an earlier version of this manuscript. I would also like to thank Zvika Brakerski and Thomas Vidick for pointing out a bug in one of my previous attempts for solving LWE made in 2022.

References

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, 2009.

[ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete gaussian sampling: Extended abstract. In *STOC*, pages 733–742. ACM, 2015.

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *STOC*, pages 99–108, 1996.

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *STOC*, pages 601–610. ACM, 2001.

[Bab86] László Babai. On lovász' lattice reduction and the nearest lattice point problem. *Comb.*, 6(1):1–13, 1986.

[Ban93] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993.

[Ban95] Wojciech Banaszczyk. Inequalities for convex bodies and polar reciprocal lattices in R^n. *Discrete & Computational Geometry*, 13(2):217–231, 1995.

[BDK+18] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In *EuroS&P*, pages 353–367. IEEE, 2018.

[BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen. Learning with errors and extrapolated dihedral cosets. In *Public Key Cryptography (2)*, volume 10770 of *Lecture Notes in Computer Science*, pages 702–727. Springer, 2018.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *STOC*, pages 575–584. ACM, 2013.

[Bri84] Ernest F Brickell. Solving low density knapsacks. In *Advances in cryptology*, pages 25–37. Springer, 1984.

[BS16] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 893–902. SIAM, 2016.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *FOCS*, pages 97–106. IEEE Computer Society, 2011.

[CCD+03] Andrew M Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 59–68, 2003.

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *EUROCRYPT (2)*, volume 9666 of *Lecture Notes in Computer Science*, pages 559–585. Springer, 2016.

[CEMM98] Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):339–354, 1998.

[CHL+23] Yilei Chen, Zihan Hu, Qipeng Liu, Han Luo, and Yaxin Tu. On the hardness of $\mathsf{S}|\mathsf{LWE}\rangle$ with gaussian and other amplitudes. *CoRR*, abs/2310.00644, 2023.

[CLZ22] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. In *EUROCRYPT (3)*, volume 13277 of *Lecture Notes in Computer Science*, pages 372–401. Springer, 2022.

[Cop97] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.*, 10(4):233–260, 1997.

[EHKS14] Kirsten Eisenträger, Sean Hallgren, Alexei Y. Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *STOC*, pages 293–302. ACM, 2014.

[FW98] Amir Fijany and Colin P Williams. Quantum wavelet transforms: Fast algorithms and complete circuits. In *NASA international conference on quantum computing and quantum communications*, pages 10–33. Springer, 1998.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, pages 169–178. ACM, 2009.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008.

[GR02] Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *arXiv preprint quant-ph/0208112*, 2002.

[Gra08] Loukas Grafakos. *Classical fourier analysis*. Springer, 2008.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

[Kan87] Ravi Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of operations research*, 12(3):415–440, 1987.

[Kit95] Alexei Y. Kitaev. Quantum measurements and the abelian stabilizer problem. 1995.

[Kup05] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.

[Len83] Hendrik Willem Lenstra. Integer programming with a fixed number of variables. *Mathematics of operations research*, 8(4):538–548, 1983.

[Liu09] Yi-Kai Liu. Quantum algorithms using the curvelet transform. In *STOC*, pages 391–400. ACM, 2009.

[LLL82] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982.

[LO85] Jeffrey C Lagarias and Andrew M Odlyzko. Solving low-density subset sum problems. *Journal of the ACM (JACM)*, 32(1):229–246, 1985.

[Mah18] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In *FOCS*, pages 332–338. IEEE Computer Society, 2018.

[MM11] Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 465–484. Springer, 2011.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pages 700–718, 2012.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measure. *SIAM Journal on Computing*, 37(1):267–302, 2007.

[MV13] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. *SIAM J. Comput.*, 42(3):1364–1391, 2013.

[NC16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016.

[NS99] Phong Q. Nguyen and Jacques Stern. The hardness of the hidden subset sum problem and its cryptographic implications. In *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 1999.

[NV08] Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *J. Math. Cryptol.*, 2(2):181–207, 2008.

[OtR85] A. M. Odlyzko and Herman J. J. te Riele. Disproof of the Mertens conjecture. *J. Reine Angew. Math.*, 357:138–160, 1985.

[Pap77] Athanasios Papoulis. *Signal analysis*. McGraw-Hill, 1977.

[Pei10] Chris Peikert. An efficient and parallel gaussian sampler for lattices. In *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 80–97. Springer, 2010.

[PRS17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. In *STOC*, pages 461–473. ACM, 2017.

[Reg04] Oded Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

[Reg23] Oded Regev. An efficient quantum factoring algorithm. *CoRR*, abs/2308.06572, 2023.

[RS17] Oded Regev and Noah Stephens-Davidowitz. A reverse minkowski theorem. In *STOC*, pages 941–953. ACM, 2017.

[Sch87] Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical computer science*, 53(2-3):201–224, 1987.

[Sha82] Adi Shamir. A polynomial time algorithm for breaking the basic merkle-hellman cryptosystem. In *CRYPTO*, pages 279–288. Plenum Press, New York, 1982.

[Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[Sim97] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

[Smi11] Julius O. Smith. *Spectral Audio Signal Processing*. `https://ccrma.stanford.edu/~jos/sasp/Fourier_Transform_Complex_Gaussian.html`, 2011. online book, 2011 edition.

[Tit51] Edward Charles Titchmarsh. *The theory of the Riemann zeta-function*. Oxford university press, 1951.