Notes on the Paper "Quantum Algorithms for Lattice Problems"
In these notes, we will introduce some of the main concepts and a short summary of the recent preprint for a quantum algorithm for solving hard lattice problems by Yilei Chen [1].

1 Complex Gaussians and Karst Waves The following is taken from [1, pp. 3-4]. Recall the Gaussian distribution $\mathcal{N}(\mu,\sigma)$ for a continuous random variable given by the probability density function

$$f(x)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{1}$$

with $\mu\in\mathbb{R}$ being the mean and $\sigma\in(0,\infty)$ being the standard deviation. The paper makes heavy use of so-called *complex Gaussian states*. We define for some $p\in\mathbb{R}_{\geq 1}$, $P\coloneqq 2^p$, qubits and $r\in\mathbb{R}_{>0}$, acting as the deviation, the *quantum Gaussian state*

$$|G_P^r\rangle\coloneqq\sum_{x=0}^{P-1}\exp\left(-\pi\frac{x^2}{r^2}\right)|x\rangle \tag{2}$$

under omission of the appropriate normalization factor.

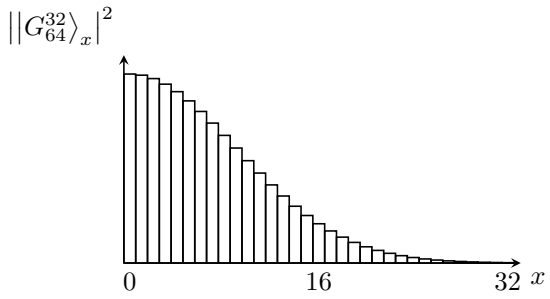

FIGURE 1. Example squared amplitude distribution of a quantum Gaussian state.

Let $s\in\mathbb{R}_{>0}$ be the standard deviation for an imaginary part of a random variable. Append a number $q\in\mathbb{N}_{\geq 1}$ of auxiliary qubits, $Q\coloneqq 2^n$. Define the unitary $U\in\mathbb{C}^{P\times P}$ with the action $|0\rangle\mapsto|G_P^r\rangle$, which can be implemented using the technique of initializing a quantum state using an efficiently integrable probability distribution by Grover and Rudolph [2]. We further define unitaries

$$U_0\colon\mathbb{C}^{PQ}\to\mathbb{C}^{PQ},|x\rangle|y\rangle\mapsto|x\rangle\left|y\oplus\mathcal{F}\left(\frac{x^2}{s^2}\right)\right\rangle \text{ and} \tag{3}$$

$$U_1\colon\mathbb{C}^{Q}\to\mathbb{C}^{Q},|x\rangle\mapsto e^{-\pi ix}|x\rangle, \tag{4}$$

where $\mathcal{F}(\cdot)$ denotes a bit representation of a floating real number. We compute

$$|0\rangle^{\otimes(p+q)}\xmapsto{U\otimes E_Q}|G_P^r\rangle|0\rangle^{\otimes q}\xmapsto{U_0}\sum_{x=0}^{P-1}\exp\left(-\pi\frac{x^2}{r^2}\right)|x\rangle\left|\frac{x^2}{s^2}\right\rangle \tag{5}$$

$$\xmapsto{U_0^\dagger(E_p\otimes U_1)}\sum_{x=0}^{P-1}\exp\left(-\pi\left(\frac{1}{r^2}+\frac{i}{s^2}\right)x^2\right)|x\rangle|0\rangle^{\otimes q}, \tag{6}$$

also referred to as employing the *Phase Kickback Trick*, all under omission of a normalization factor. implicitly defining the *complex quantum Gaussian state* $|G_P^{r,s}\rangle$. The parameters r and s control the spread of the real and imaginary parts of the amplitudes.

Perform

$$|G_P^{r,s}\rangle \xmapsto{\mathrm{QFT}_P} \frac{1}{\sqrt{P}} \sum_{y=0}^{P-1} \sum_{x=0}^{P-1} \exp\left(-\pi \left(\frac{1}{r^2} + \frac{i}{s^2}\right) x^2\right) \exp\left(-2\pi i \frac{xy}{P}\right) |y\rangle \,. \tag{7}$$

It can be proven that the amplitudes of the resulting state concentrate on values of y, which approximately lay on $\alpha\mathbb{Z}$ for some $\alpha \in \mathbb{R}_{>0}$. The behavior of the real parts of the amplitudes is why they are referred to as *Karst Waves*, see Figure 2, resembling geological Karst formations, see Figure 3.

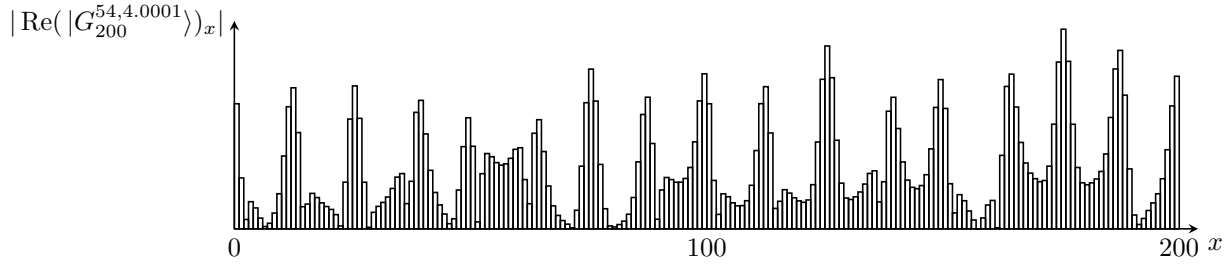

FIGURE 2. Absolute values of the real parts of the amplitudes of $|G_{200}^{54,4.0001}\rangle$, parameters taken from [1, p. 5].

FIGURE 3. Example of Karst formations in Guilin, China, see [3].

2 Windowing with States The following is due to [1, pp. 4-6]. *Windowing* is a technique of combining two quantum states in a *convolution*-type manner. The technique works as follows: Suppose two states

$$|\Phi\rangle \coloneqq \sum_{x=0}^{P-1} \Phi_x |x\rangle \text{ and } |\Psi\rangle \coloneqq \sum_{y=0}^{Q-1} \Psi_y |y\rangle \tag{8}$$

are given. We tensorize both states and perform

$$|\Phi\rangle \otimes |\Psi\rangle \xmapsto{U_{\mathrm{Id}}} \sum_{x=0}^{P-1} \sum_{y=0}^{Q-1} \Phi_x \Psi_y |x\rangle |x+y \bmod P\rangle \xmapsto{E_P \otimes \not\Delta} \sum_{x=0}^{P-1} \Phi_x \Psi_{y'-x \bmod Q} |x\rangle |y'\rangle \tag{9}$$

with some $y' = x + y \bmod Q$, the state obtained is the result.

3 Algorithm Outline Recall the LWE (Learning With Errors) problem. On a high level, the task is to find a secret vector, whose entries are sampled from a distribution. Solving LWE in polynomial time gives polynomial algorithms for the SVP (Shortest Vector Problem) and its variants [1, pp. 1-2].

1. In the algorithms preparatory phase, a given LWE instance is converted into a version with some chosen error terms following a secret distribution and then into a so-called *q-ary lattice with a unique shortest vector* [1, pp. 14–18], where $q \in \mathbb{N}$. These reductions give a problem that is as hard to solve as normal LWE. Thus, the reduction roughly follows the strategy SVP $\leq$ LWE $\leq$ SVP. The "q-ary" part of the lattice name implies the use of $\mathbb{Z}_q$ to make the lattice finite for the algorithm, as a quantum register will be used to store a complex Gaussian superposition over the lattice.
2. The preparation for the algorithm ends with a comprehensive parameter selection [1, pp. 18-20].
3. The main quantum algorithm consists of nine steps. In the first seven steps, an imaginary Gaussian state based on a superposition of the q-ary lattice is windowed with a special auxiliary state and processed further [1, pp. 20-31].
4. The result is then reduced to a linear system of equations over a finite field, which is supposed to yield the LWE solution [1, pp. 31-39].

Table 1. Extended Paper Overview

PDF Page	Description
1-2	Abstract, Comment and Contents
3-5	Definitions of SVP, GapSVP, SIVP and LWE
5-8	Complex Gaussians
8-10	Reduced algorithm overview, very sparse on inner workings.
10-11	Preliminaries: Math
12-14	Preliminaries: Lattices
14-16	Preliminaries: Quantum Computation
16-22	Transform LWE in three steps: First with k known secrets by essentially adding k entries to the search vector, then into a q-ary SVP and then select parameters appropriately.
22-24	Detailed Quantum Algorithm Description
24-40	Description of Steps
39	Bug
41-65	Detailed proofs, further discussions, acknowledgements and references

We will not go into further detail here, but we will give a short description of the technique involved in the claimed problem of the algorithms analysis discovered on April 18, 2024.

For that, we consider another technique used, called *domain extension* [1, p. 14]. Suppose we are given a P-periodic function $f\colon \mathbb{Z} \to \mathbb{C}$ with $f(\mathbb{Z}_P) \neq \{0\}$. Define

$$|\phi\rangle \coloneqq \sum_{x=0}^{P-1} f(x)\,|x\rangle\,, \tag{10}$$

again omitting a normalization factor. Let $c \in \mathbb{N}_{\geq 1}$, $C \coloneqq 2^c$. We perform

$$|0\rangle^{\otimes c}\,|\phi\rangle \xmapsto{H^{\otimes c}\otimes E_P} \frac{1}{\sqrt{C}} \sum_{h=0}^{C-1}\sum_{x=0}^{P-1} f(x)\,|h\rangle\,|x\rangle \tag{11}$$

$$= \frac{1}{\sqrt{C}} \sum_{h=0}^{C-1}\sum_{x=0}^{P-1} f(hP+x)\,|hP+x\rangle = \frac{1}{\sqrt{C}} \sum_{x=0}^{CP-1} f(x)\,|x\rangle\,, \tag{12}$$

naturally extending the state from a superposition over $\mathbb{Z}_P$ with amplitudes based on f to an analogous state over $\mathbb{Z}_{CP}$.

The algorithms analysis is claimed to fail due to a wrong application of the domain extension technique in step 9 [1, pp. 34-38].

4 Further Perspectives We have discussed four techniques used in the paper by Yilei:

- Real and complex Gaussian states
- Karst wave states
- Windowing states
- Domain extension

Based on them, we will now discuss some possible directions and some more aspects to the algorithm.

Let $t \in \mathbb{N}_{\geq 1}$, $T \coloneqq 2^t$. In the original HHL algorithm, an auxiliary state

$$\sqrt{\frac{2}{T}} \sum_{\tau=0}^{T-1} \sin\left(\frac{\pi(\tau + \frac{1}{2})}{T}\right) |\tau\rangle \tag{13}$$

was initialized at the beginning of the algorithm [4, p. 2]. It helps with obtaining good approximations of the given Hamiltonians energies/eigenvalues. Comparing Figure 4, a sketch of the amplitudes of an example of this state, and Figure 1, we recognize the similarity, the former should imitate a general real Gaussian state. I proposed this interpretation between 2021-2022.

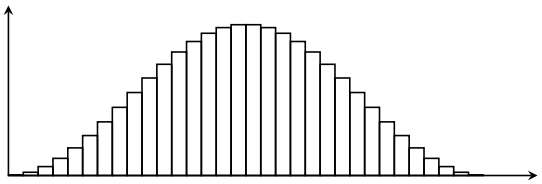

FIGURE 4. Sketch of the amplitudes taken from [5, p. 31], here for $t = 5$ and scaled by 16.

One might now ask the question if the original HHL algorithm is faster with a specifically chosen real or imaginary Gaussian quantum state.

In terms of adiabatic quantum computation, one could study rapidly changing, Karst wave like, energy changes following the pattern of Figure 2. There are no results on this yet, besides the trivial action of speeding up the adiabatic schedule employed. Fast changes of certain submatrices of a Hamiltonian might lead to an effect similar to the Zeno effect, effectively yielding an adiabatic version of the independent development of parts of a state, presenting a, possibly easier to control, alternative to the measurement-based Zeno.

Windowing states may be useful for quantum machine learning - as it presents a natural version of convolution, as discussed above - or for techniques involving the modelling of an exponential number of signal samples using a quantum state, i.e., performing classical signal processing using a quantum state. There may exist results on this already. By the concept, and as complex Gaussian states, which are very important in general signal processing, have already been employed, it only seems natural to use the technique for this kind of signal processing.

Domain extension does not seem to be an interesting technique in general, as it boils down to extending the domain of a periodic function, while it naturally keeps its image.

As for the paper itself, work seems to have stopped fully, as indicated by Yileis note on the front page [1]. Whilst the multiple techniques employed and the complexity of the arguments involved are intruiging, the paper fails to communicate the intuition and inner workings behind the proposed algorithm. Also, the fact

that one application of domain extensions leads to the algorithm failing seems very strange, considering that domain extension does not add much information to a state, as discussed above.

For now, following Yilei, it does not seem that the proposed result is still achievable due the bug. One possible opportunity for getting more people to work on it may be rewriting parts of the paper into a more pedagogical version, more clearly establishing notation (maybe by a notation table) and focusing more on the intuition behind the algorithm instead of its associated large formulas.

References

[1] Y. Chen, *Quantum Algorithms for Lattice Problems*, [Accessed: 19.07.2024, 11:22]. [Online]. Available: https://eprint.iacr.org/2024/555.

[2] L. Grover and T. Rudolph, "Creating superpositions that correspond to efficiently integrable probability distributions," DOI: 10.48550/arXiv.quant-ph/0208112.

[3] Wikipedia. "Lijiang fengcong (cone karst) in Guilin as part of the South China Karst." [Accessed: 21.07.2024, 14:29]. (), [Online]. Available: https://upload.wikimedia.org/wikipedia/commons/0/06/87340-Li-River_(29881879337).jpg.

[4] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for solving linear systems of equations," DOI: 10.48550/arXiv.0811.3171.

[5] valentinpi. "Bachelor-Thesis: A Comprehensive Description of the Quantum HHL Algorithm and its Application in the Cryptanalysis of the AES." [Accessed: 22.07.2024, 23:20]. (), [Online]. Available: https://valentinpi.github.io/posts/bachelor-thesis/bachelor_thesis.pdf.