A Note on Quantum Algorithms for Lattice Problems

Omri Shmueli*

Recently, a paper [Che24] by Chen has claimed to construct a quantum polynomial-time algorithm that solves the Learning With Errors (LWE) Problem [Reg09], for a range of parameters. As a byproduct of Chen's result, it follows that Chen's algorithm solves the Gap Shortest Vector Problem $\mathsf{GapSVP}_{g(n)}$ for gap $g(n) = \tilde{O}\left(n^{4.5}\right)$, by using Regev's quantum polynomial-time reduction [Reg09] from (some parameters of) GapSVP to LWE. In this short note we point to an error in the claims of Chen's paper.

The algorithm is presented in Sections 3.4, 3.5, 3.6 and 3.7 of [Che24]. The algorithm's correctness is conditioned on the parameter selection, detailed in Section 3.3 and in the beginning of Section 3.2 of the paper. Our observation is very simple and can be summed up as that the parameter choices are impossible. To elaborate, as part of the parameter choices detailed at the beginning of Section 3.2, the author sets two choices:

- A number $\kappa \in \mathbb{N}$ such that $\kappa \in O(\log n)$.
- κ numbers $p_1, \cdots, p_\kappa \in \mathbb{N}$, such that the κ numbers are (1) pairwise coprime, and (1) all numbers are bounded by $\log(n)$.

We claim that there exist $\kappa \in \Omega(\log(n))$ such that for large enough parameter n, there does not exist such sequence of κ numbers $p_1, \cdots p_\kappa$, this explicitly violates, for example, the conditions of Lemma 3.6. in the paper. We provide a proof to our claim regarding the impossibility for the algorithm's parameters.

Claim 0.1. *Let $\kappa(n) := \kappa$ any function of n such that $\kappa(n) \in \omega\left(\frac{\log(n)}{\log(\log(n))}\right)$. Then, for a sufficiently large n, there does not exist $\kappa(n)$ numbers $p_1, \cdots, p_\kappa \in \mathbb{N}$ such that all numbers are pairwise coprime, and also $\forall i \in \{1, 2, \cdots, \kappa\}$,$p_i \leq \log(n)$.*

Proof. Let $\kappa := \kappa(n)$ as above and let $p_1, \cdots, p_\kappa \in \mathbb{N}$ such that all κ numbers are pairwise coprime. Assume without the loss of generality that the numbers are in an ascending order $p_1 < \cdots < p_\kappa$. We will show that necessarily $p_\kappa > \log(n)$. Next, let $q_1, \cdots, q_\kappa$ be the first κ primes numbers, that is, $q_1 = 2$, $q_2 = 3$, $q_3 = 5$ and so on.

We claim that it is necessarily the case that $q_\kappa \leq p_\kappa$: First, note that for the pairwise coprime numbers $p_1 \cdots, p_\kappa$, there is no prime number which is a factor of two different p_i, p_j for $i \neq j$, by definition. Next, we define a sequence of prime numbers $\tilde{p}_1 < \cdots < \tilde{p}_\kappa$ as follows: The number $\tilde{p}_1$ is the smallest prime factor in the set of prime factors of $p_1 \cdots, p_\kappa$. For each $i \in \{2, \cdots, \kappa\}$, the number $\tilde{p}_i$ the prime factor in the set of prime factors of $p_1 \cdots, p_\kappa$, which is (a) bigger than the previous $\tilde{p}_{i-1}$ and also (b) not a prime factor of the same number for which $\tilde{p}_{i-1}$ is a prime factor. Finally, observe that (1) $\tilde{p}_\kappa \leq p_\kappa$ and also (2) $q_\kappa \leq \tilde{p}_\kappa$.

It remains to only show that $q_\kappa > \log(n)$, so assume towards contradiction $q_\kappa \leq \log(n)$. By the prime numbers theorem, we have the limit

$$\lim_{m \to \infty} \frac{\pi(m)}{\left(\frac{m}{\ln(m)}\right)} = 1 \ ,$$

[*] Tel Aviv University, omrishmueli@mail.tau.ac.il. Supported in part by the European Research Council (ERC) under the European Union's Horizon Europe research and innovation programme (grant agreement No. 101042417, acronym SPP), and by the Clore Israel Foundation.

where π is the prime-counting function, that is, $\pi(m)$ is the number of prime numbers between 1 and m. From the above limit it follows that for a sufficiently large $n \in \mathbb{N}$, the number of prime numbers between 1 and $\log(n)$ is $\leq c \cdot \frac{\log(n)}{\ln(\log(n))}$ for some absolute positive constant $c \in \mathbb{R}_{>0}$. However, $\kappa \in \omega\left(\frac{\log(n)}{\log(\log(n))}\right)$, which means q_κ cannot be bounded by $\log(n)$, because if it was, then there would be more than $c \cdot \frac{\log(n)}{\ln(\log(n))}$ prime numbers between 1 and $\log(n)$. $\square$

We conclude this note with two main takeaways.

- Our claim only invalidates the current version of the paper. If it is possible to take $\kappa = O\left(\frac{\log(n)}{\log(\log(n))}\right)$ and the algorithm is proven to still work, or to make other changes to the algorithm such that there is no need for such sequence of pairwise coprime numbers, our claims for incorrectness do not hold anymore.

- In case (1) there is no immediate fix to the algorithm's parameters, and also (2) the rest of the results in the paper are correct, this means that the only thing preventing the existence of a quantum polynomial-time algorithm for the LWE problem (and other lattice problems), is the fact that there are not enough primes between 1 and $\log(n)$. If this is the case, we find it as an extremely interesting consequence of Chen's work.

References

[Che24] Yilei Chen. Quantum algorithms for lattice problems. *Cryptology ePrint Archive*, 2024.

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