

A noise robust approach for solving the state hidden subgroup problem on cyclic groups with a quantum computer

Adrián Pérez-Salinas,^{1,2} José Carrasco,¹ and Jens Eisert¹

¹*Dahlem Center for Complex Quantum Systems – Freie Universität Berlin, Germany*

²*Institute for Theoretical Physics – ETH Zürich, Switzerland*

Quantum computers are devices equipped with enhanced capabilities to process information, as compared to digital (or classical) computers. These enhanced capabilities have been experimentally demonstrated even on imperfect quantum devices [1–5]. For running some interesting problems with theoretical advantages, such as Shor’s celebrated integer factorization algorithm [6], fault-tolerant devices are required. Shor’s algorithm falls into a wider class of problems known as the hidden subgroup problem (HSP), where advantages have been thoroughly examined [7–9], including in the field of QML [10, 11]. For quantum computers, the HSP is more naturally addressable in its state version – StateHSP –, where the hidden information of the subgroup is encoded in a quantum state [12, 13]. An important caveat of the (State)HSP is that any sampling error might destroy all signal from the quantum computer, making the procedure extremely sensitive to errors.

In this work, we revisit the StateHSP on abelian cyclic groups and propose a method to solve it that exhibits robustness against noise. Our method uses classical post-processing of drawn samples to increase their statistical significance and distinguish signal from the hidden subgroup and noise arising from random outcomes. Such post-processing is rooted in number theory, more specifically on the structure of the primes. The post-processing is based on the use of the greatest common divisor (gcd), which admits efficient classical computation. The gcd procedure gives robustness to the hidden subgroup to be unveiled from samples. Our work presents analytical guarantees for global and local depolarizing noises. However, the concentration of samples under our post-processing is qualitatively significant to expect similar behavior under more general noise models. As a byproduct, this method yields constant runtime on the size of the group, improving the previous scaling $\mathcal{O}(\log |G|)$.

The main observation needed to find the post-processing is the concentration of divisors of integers, which implies strong concentration in the gcd.

$$\lim_{N \rightarrow \infty} \mathbb{P}(p^k | n) = \lim_{N \rightarrow \infty} \mathbb{P}(\nu_p(n) \geq k) = p^{-k} \implies \lim_{N \rightarrow \infty} \mathbb{P}(\gcd(n_1, n_2) = K) = \frac{6}{\pi^2} \frac{1}{K^2}. \quad (1)$$

This observation is useful to unveil the hidden subgroup in a (State)HSP for cyclic groups. For a group $\mathbb{Z}_N$, any subgroup is defined by a factor q that divides N . A noiseless Fourier sampling on the HSP allows to return samples λ such that $q\lambda = 0 \pmod{N}$. Hence, in order to identify the group, it suffices to find the smallest value of λ that satisfy this constraint. This allows us to find the correct subgroup with probability at least $1 - \delta$ using a number of samples scaling as $M \in \Theta(\log \delta^{-1})$, in contrast to previous group-size-dependent scalings [12, 13]. The root for this speed-up is the use of a probabilistic approach based on Equation (1).

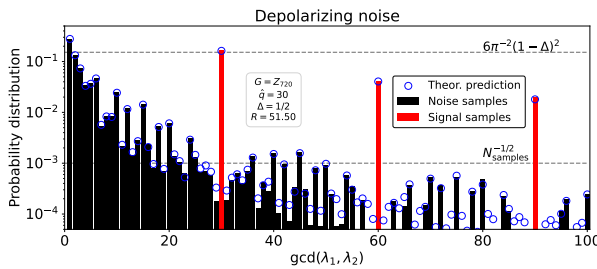


FIG. 1: Signal (red) and noise (black), together with theoretical predictions (blue circles) for the cyclic group $\mathbb{Z}_{720}$, with the hidden subgroup $24\mathbb{Z}_{720}$ and depolarizing noise Δ .

When noisy outcomes are considered, it is possible to exploit the strong concentration from Equation (1) to statistically extract a signal from the noisy samples. While the analytical results are lengthy to present, they exhibit a clear distinction between signal and noise, as visible in Figure 1. In this scenario, signals stand out from a noisy background and allow for efficient identification. Further work is required to extend the present results to more general abelian groups, although we conjecture through numerical explorations that the concentration argument will suffice to obtain similar results also in the generic abelian group.

This procedure gives robustness to the StateHSP problem and opens a path for reducing the fault-tolerance requirements of quantum computers to address it. For instance, the use of perfect oracle states is

no longer needed. Fields like quantum machine learning can benefit from this relaxation and find candidate solutions to learning problems in the realistic cases where the data meets the StateHSP only approximately.

-
- [1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, et al., *Nature* **574**, 505 (2019), ISSN 1476-4687.
 - [2] S. Aaronson and A. Arkhipov, *The Computational Complexity of Linear Optics* (2010), 1011.3245.
 - [3] S. Aaronson and L. Chen, *Complexity-Theoretic Foundations of Quantum Supremacy Experiments* (2016), 1612.05903.
 - [4] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, et al., *Science* **370**, 1460 (2020), ISSN 0036-8075, 1095-9203.
 - [5] M. J. Bremner, R. Jozsa, and D. J. Shepherd, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **467**, 459 (2011), ISSN 1364-5021, 1471-2946, 1005.1407.
 - [6] P. W. Shor, *SIAM Journal on Computing* **26**, 1484 (1997), ISSN 0097-5397.
 - [7] M. Ettinger and P. Høyer, *Advances in Applied Mathematics* **25**, 239 (2000), ISSN 01968858.
 - [8] M. J. Kearns and U. Vazirani, *An Introduction to Computational Learning Theory* (The MIT Press, 1994), ISBN 978-0-262-27686-3.
 - [9] M. Blum and S. Micali, *SIAM Journal on Computing* **13**, 850 (1984), ISSN 0097-5397, 1095-7111.
 - [10] C. Gyurik and V. Dunjko, *Exponential separations between classical and quantum learners* (2023), 2306.16028.
 - [11] Y. Liu, S. Arunachalam, and K. Temme, *Nature Physics* **17**, 1013 (2021), ISSN 1745-2481.
 - [12] M. Hinsche, J. Eisert, and J. Carrasco, *The abelian state hidden subgroup problem: Learning stabilizer groups and beyond* (2025), 2505.15770.
 - [13] D. Wakeham and M. Schuld, *Inference, interference and invariance: How the Quantum Fourier Transform can help to learn from data* (2024), 2409.00172.