

Research Proposal - Fault-Tolerant Shallow Circuits.

Michael Ben-Or David Ponomarev

July 9, 2025

Abstract

We study the overall depth overhead cost required for constructing fault-tolerant circuits. We focus on shallow depth circuit classes, in particular, \mathbf{QAC}_0 , $\mathbf{QNC}_{0,f}$, \mathbf{QNC}_1 , and 'QNC without reset gates', and certain known problem candidates for demonstrating quantum advantage such as factoring [Sho97] and Instantaneous Quantum Polynomial-time [BMS17], [Pal+24]. We aim to answer whether there exists a fault tolerance with only constant overhead at the circuit's depth. A positive answer implies that computing logarithmic depth circuits when subjected to noise is not harder than computing in an ideal environment.

1 Introduction.

The Quantum Computation model is widely believed to be superior to classical models, offering asymptotic speedup in tasks such as factoring [Sho97], searching [Gro96], simulating, and more relative to the best-known classical solutions. Yet even though there is almost complete agreement about the superiority of the ideal quantum model, there is still a debate over whether it is possible to implement complex computation in the real world, where the qubits and gates are subject to faults. Similarly, the feasibility of realizing classical computation has also been an open question. In fact the question about the feasibility of computation under noise is almost as ancient as the computer science field itself, initialized by Von Neumann [Neu56] at the time that classical computation putted in debuts. Time been pass and the followed works had pointed that not even a polynomial computation in the presence of noise is still reasonable but one can implement a fault tolerance version at a most constant times cost at the circuits depth [Pip85]. Or in asymptotic sense, classical computation in the presence of noise is as exactly hard as computation in ideal environment.

Recently, the feasibility question has been raised again, this time regarding quantum computing, and while an intensive work has been done, and also succeed to prove that polynomial quantum computation can be made fault tolerance, [AB99],[Got14] and even with only constant overhead at the original circuit width [Gro19], the required depth overhead is still not well understood. We stress out that in all the familiar constructions, in construct to Pippenger [Pip85], original constant-depth gates are mapped to asymptotically grow¹ depth gates.

Moreover, even the depth overhead is particularly interesting as today's quantum machines are challenged to maintain quantum states for a long time [CITE]. The limitations of these machines have motivated research to define NISQ, which stands for Noisy Intermediate-Scale Quantum, referring to the current era of quantum computing characterized by quantum processors that have a limited number of qubits and are prone to errors due to noise. In addition to NISQ, another common characterization for limited quantum computation is computation without reset gates, which has been proved to be impossible when restricted to polynomial space [Aha+96]. Having a constant depth-overhead fault tolerance scheme would imply the feasibility of log depth computation in that model.

This work addresses the above. We ask whether a magnitude depth overhead is an unavoidable price that one has to pay, If a Constant Depth Fault Tolerance Construction (CDFT) exists, and if so, how to construct it. In particular, whether an ideal \mathbf{QNC}_1 , the class of problems that can be decided by logarithmic depth quantum circuits, can be computed in noisy- \mathbf{QNC}_1 circuits.

¹Note, that here, classical computation is also counted in the overall depth cost

Additionally, we extend the question beyond the standard classes and ask about fault-tolerant sampling. Specifically, we consider several sampling processes by shallow quantum circuits, which are believed to be infeasible for classical circuits, such as Instantaneous Quantum Polynomial-time [BMS17], [Pal+24], and ask about the depth efficiency of their fault-tolerant version.

The proposal is organized as follows. Section 2 presents the notations, formal definitions, and states the open problems that will be studied through the research. Then, Section 3 describes strategies to prove CDFT. In particular, it lists primitives that can be used to achieve it and discusses how far we are from obtaining them. Having said that, Section 4 presents the first cues against the possibility of CDFT and provides the entry points to prove the impossibility claim. Finally, Section 5 discusses the applications and implications of either the correctness of CDFT or the impossibility of CDFT, from both theoretical and practical views.

2 Notations.

In the following, we present the notations used in the paper. Readers who are familiar with the literature of coding theory and quantum fault tolerance might skip ?? and ?? and continue directly to ??, which introduces less standard notations.

Definition 2.1 (NC - Nick’s Class). NC_i is the class of decision problems solvable by a uniform family of Boolean circuits, with polynomial size, depth $O(\log^i(n))$, and fan-in 2.

Definition 2.2 (QNC). The class of decision problems solvable by polylogarithmic-depth, and finite fan out/in quantum circuits with bounded probability of error. Similarly to NC_i , QNC_i is the class where the circuits have $\log^i(n)$ depth.

Definition 2.3 (QNC_G). For a fixing finite fan in/out gateset G , the class with deciding circuits composed only for gates in G and at depth at most polylogarithmic. And in similar to QNC_i , $\text{QNC}_{G,i}$ is the restriction to circuits with depth at most $\log^i(n)$.

3 Strategies to get CDFT.

4 Cues against CDFT.

5 Applications.

References

- [Neu56] J. von Neumann. “Probabilistic Logics and the Synthesis of Reliable Organisms From Unreliable Components”. In: *Automata Studies*. Ed. by C. E. Shannon and J. McCarthy. Princeton: Princeton University Press, 1956, pp. 43–98. ISBN: 9781400882618. DOI: [doi:10.1515/9781400882618-003](https://doi.org/10.1515/9781400882618-003). URL: <https://doi.org/10.1515/9781400882618-003>.
- [Pip85] Nicholas Pippenger. “On networks of noisy gates”. In: *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*. 1985, pp. 30–38. DOI: [10.1109/SFCS.1985.41](https://doi.org/10.1109/SFCS.1985.41).
- [Aha+96] D. Aharonov et al. *Limitations of Noisy Reversible Computation*. 1996. arXiv: [quant-ph/9611028](https://arxiv.org/abs/quant-ph/9611028) [quant-ph]. URL: <https://arxiv.org/abs/quant-ph/9611028>.
- [Gro96] Lov K. Grover. *A fast quantum mechanical algorithm for database search*. 1996. arXiv: [quant-ph/9605043](https://arxiv.org/abs/quant-ph/9605043) [quant-ph].
- [Sho97] Peter W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. DOI: [10.1137/S0097539795293172](https://doi.org/10.1137/S0097539795293172). URL: <https://doi.org/10.1137/S0097539795293172>.

- [AB99] Dorit Aharonov and Michael Ben-Or. *Fault-Tolerant Quantum Computation With Constant Error Rate*. 1999. arXiv: [quant-ph/9906129](#) [[quant-ph](#)].
- [Got14] Daniel Gottesman. *Fault-Tolerant Quantum Computation with Constant Overhead*. 2014. arXiv: [1310.2984](#) [[quant-ph](#)].
- [BMS17] Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. “Achieving quantum supremacy with sparse and noisy commuting quantum computations”. In: *Quantum* 1 (Apr. 2017), p. 8. ISSN: 2521-327X. DOI: [10.22331/q-2017-04-25-8](#). URL: <https://doi.org/10.22331/q-2017-04-25-8>.
- [Gro19] Antoine Grospellier. “Constant time decoding of quantum expander codes and application to fault-tolerant quantum computation”. Theses. Sorbonne Université, Nov. 2019. URL: <https://theses.hal.science/tel-03364419>.
- [Pal+24] Louis Paletta et al. “Robust sparse IQP sampling in constant depth”. In: *Quantum* 8 (May 2024), p. 1337. ISSN: 2521-327X. DOI: [10.22331/q-2024-05-06-1337](#). URL: <https://doi.org/10.22331/q-2024-05-06-1337>.