

# On The Cost of Fault-Tolerant Shallow Circuits.

Michael Ben-Or David Ponomarevsky

November 7, 2024

## Abstract

In this work we study the overall depth overhead cost required for constructing fault tolerance circuits. We focus on shallow depth circuits classes, In particular,  $\mathbf{QAC}_0$ ,  $\mathbf{QNC}_{0,f}$  and  $\mathbf{QNC}_1$  and certain known problem candidates for demonstrating quantum advantage such as factoring [Sho97] and Instantaneous Quantum Polynomial-time [BMS17], [Pal+24]. We only give a partial answers, Yet, clues that might pave the way towards a full understanding the complexity versus fault tolerance trade-off.

## 1 Introduction.

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. Although

## 2 Todo:

1. Move to encoding each qubit by logarithmic width (instead of chunks) the reason is that the gate teleportation becomes complicated when it applied over higher dimension.
2. Then showing for 2-qubit gates set that is indeed works.
3. Treating separately to noise observed in two qubits gates.

## 3 Fault tolerance Toffoli.

[COMMENT] In that section the  $\cdot$  operation is the pair wise product (pair wise AND).

Assume that  $\bar{0}, \bar{1} \in C_X$  and that they belong to two different cosets of  $C_X/C_Z^\perp$ . Let  $x, y \in \{\bar{0}, \bar{1}\}$ .

$$\begin{aligned} & \sum_{z, z', w \in C_Z^\perp} |z\rangle |z'\rangle |w\rangle \\ & \sum_{z, z', w \in C_Z^\perp} |z\rangle |z'\rangle |w + z \cdot z'\rangle \\ & \sum_{z, z', w \in C_Z^\perp} |z + x\rangle |z' + y\rangle |w + z \cdot z'\rangle \\ & \sum_{z, z', w \in C_Z^\perp} |z + x\rangle |z' + y\rangle |x \cdot y + x \cdot z' + y \cdot z + z z' + w + z \cdot z'\rangle \\ & \sum_{z, z', w \in C_Z^\perp} |z + x\rangle |z' + y\rangle |x \cdot y + x \cdot z' + y \cdot z + w\rangle \end{aligned} \tag{1}$$

Since  $x, y \in \{\bar{0}, \bar{1}\}$  we have that  $x \cdot z'$  equals to either  $z'$  or  $\bar{0}$ . Hence  $\sum_{w \in C_Z^\perp} |\xi + x \cdot z + w\rangle = \sum_{w \in C_Z^\perp} |\xi + w\rangle$ . So the idea is the following, suppose that one has to compute Toffoli at time  $t$  over the

registers  $R_1, R_2, R_3$ . First, at time 0, he initialize a logical zero  $|C_Z^\perp\rangle$  in each register, then he compute pairwise Toffoli  $R_1, R_2$  into  $R_3$ . That gives the ket  $\sum_{z, z', w \in C_Z^\perp} |z \cdot z' + w\rangle$ , immediately afterwards encode  $R_3$  again into a good quantum code. Denote by  $\tau$  the time required for decoding  $R_3$  back, at time  $t - \tau$  start to decode  $R_3$ . Eventually at time  $t$  compute again the transversal Toffoli, by Equation (1) we gets the desired.

By similar arguments exhibited at Claim 6.3 one can show that the errors behaves according to a Pauli noise channel. **[COMMENT]** That is not correct, since the concatenation construction assumes that all the registers initialized to physical zeros in the begging of the computation.

### 3.1 Another Idea, $z \cdot z'$ can't contribute too mach.

Clearly we have that  $|z \cdot z'| \leq |z|, |z'|$  therefore we have that  $\Pr_{z, z' \in C_Z^\perp} [|z \cdot z'| \geq t] \leq \Pr_{z \in C_Z^\perp} [|z| \geq t]$ . Now assume that the tanner code by which the code defined is bipartite graph and denote by  $z_+, z_-$  the grouping of the  $z$ 's generators supported on the even and the odd vertices of the graph. By triangle inequality  $|z| = |z_+ + z_-| \leq |z_+| + |z_-|$ . So if  $|z| > t$  then at least one of  $|z_-|, |z_+|$  is greater than  $t/2$ . Hence via the union bound:

$$\Pr_{z \in C_Z^\perp} [|z|] \leq \Pr_{z \in C_Z^\perp} \left[ \bigcup_{i \in \pm} |z_i| \geq t/2 \right] \leq \sum_{i \in \pm} \Pr_{z \in C_Z^\perp} [|z_i| \geq t/2]$$

Since any two positive (negative) generators are disjoint we have that  $|z_+|$  is a sum of the independent random variables each stands for the weight contributed by a positive vertex. Let us denote by  $V^+, V^-$  the positive and the negative vertices and for each vertex  $v \in V$  we will denote by  $z_v$  the bits of  $z$  restricted to  $v$  edges. So  $|z_\pm| = \sum_{v \in V^\pm} |z_v|$ . For simplicity assume that  $|V^+| = |V^-| = n/2$  and that  $\mathbf{E}_{z \in C_A \otimes C_B} [|z|] = \mu$ . Then we can use concentration inequality to have:

$$\Pr_{z \in C_Z^\perp} [|z|] \leq \sum_{i \in \pm} \Pr_{z \in C_Z^\perp} \left[ \sum_{v \in V^i} |z_v| \geq t/2 \right] \leq 2e^{-(\mu - \frac{t}{2})n}$$

Thus if  $\mu - \gamma \geq O(1)$  (from Claim 6.2) then with high probability the Toffoli is computed up to reducible error.

## 4 Notations.

We denote by  $C_g$  the good qLDPC code [Din+22] [PK21] [LZ22b], and by  $C_{ft}$  the concatenation code presented at [AB99] ( $ft$  stands for fault tolerance). For a code  $C_y$ , we use  $\Phi_y, E_y, D_y$  to denote the channel maps circuits into the their matched circuits compute in the code space, the encoder, and the decoder, respectively. We use  $\Phi_U$  to denote the 'Bell'-state storing the gate  $U$ . We say that a state  $|\psi\rangle$  is at a distance  $d$  from a quantum code  $C$  if there exists an operator  $U$  that sends  $|\psi\rangle$  into  $C$  such that  $U$  is spanned on Paulis with a degree of at most  $d$ . Sometimes, when the code being used is clear from the context, we will say that a block  $B$  of qubits has absorbed at most  $d$  noise if the state encoded on  $B$  is at a distance of at most  $d$  from that code.

## 5 The Noise Model

### 6 Fault Tolerance (With Resets gates) at Linear Depth.

**Claim 6.1.** *There exists a value  $p_{th} \in (0, 1)$  such that if  $p < p_{th}$ , then any quantum circuit  $C$  with a depth of  $D$  and a width of  $W$  can be computed by a  $p$ -noisy circuit  $C'$ , which allows for resets. The depth of  $C'$  is at most  $\max\{O(D), O(\log(WD))\}$ .*

#### 6.1 Initializing Magic for Teleportation gates and encodes ancillaries.

The Protocol:

1. Initialization of zeros: The qubits are divided into blocks of size  $|B|$ . Each block is encoded in  $C_g$  using  $D_{ft} \Phi_{ft}[E_g] |0^{|B|}\rangle$ .

2. Initialization of Magic for Teleportation gates: The gates in the original circuit are encoded in  $C_g$  using  $D_{ft}\Phi_{ft}[E_g]|\Phi_U\rangle$ .
3. Gate teleportation: Each gate in the original circuit is replaced by a gate teleportation.
4. Error reduction: After the initialization step, at each time tick, each block runs a single round of error reduction.

**Claim 6.2** (From [LZ22a]). *Assuming that an error  $|e| \leq \gamma n$ , i.e  $e$  is supported on less than  $\gamma n$  bits, then a single correction round reduce  $e$  to an error  $e'$  such that  $|e'| < \nu|e|$ .*

**Claim 6.3.** *The gate  $D_{ft}\Phi_{ft}[E_g]$  initializes states encoded in  $C_g$  subject to a  $3p$ -noise channel.*

*Proof.* Clearly, with high probability,  $\Phi_{ft}[E_g]$  successfully encodes into  $C_{ft} \circ C_g$ , let's say with probability  $1 - \frac{1}{\text{poly}(n)}$ . Denote by  $E_i$  and  $D_i$  the encoder and decoder at the  $i$ th level of the concatenation construction. Consider the decoder under  $\mathcal{N}$  action:  $P_2 D_1 P_2 D_2, \dots, P_{i-1} D_i P_i$ , by the fault-tolerance construction, a logical error at the  $i$ th stage occurs with probability  $p^{2^i}$ . Therefore, by the union bound, the probability that in one of the steps the circuit absorbs an error that is not corrected is less than  $p + p^2 + p^4 + \dots < 2p$ . Hence, any decoded qubit absorbs noise with probability less than  $2p$ .

Thus, overall, we can bound the probability of a single qubit being faulty by:

$$\begin{aligned} \Pr[\text{fault}] &= \Pr[\text{fault}|\Phi_{ft}[E_g]] \cdot \Pr[\Phi_{ft}[E_g]] + \Pr[\text{fault}|\overline{\Phi_{ft}[E_g]}] \cdot \Pr[\overline{\Phi_{ft}[E_g]}] \\ &\leq \Pr[\text{fault}|\Phi_{ft}[E_g]] + \Pr[\overline{\Phi_{ft}[E_g]}] \leq 2p + \frac{1}{\text{poly}(n)} \leq 3p \end{aligned}$$

**Remark 6.1.** *In our construction, we use the concatenation code to encode blocks of length  $\log(n)$ . Therefore, any  $\text{poly}(n)$  in the above should be replaced by  $\log(n)$ . However, this does not affect anything since the inequality does not depend on  $n$ .*

□

**Claim 6.4.** *With a probability  $1 - \frac{WD}{|B|} \cdot D2e^{-2|B|(\beta-p)}$ , the total amount of noise absorbed in a block at any given time  $t$ , is less than  $\gamma n$ .*

*Proof.* Consider the  $i$ th block, denoted by  $B_i$ . By applying Hoeffding's inequality, we have that the probability that more than  $\beta|B|$  qubits are flipped at time  $t$  is less than  $2e^{-2|B|(\beta-p)}$ . By using the union bound over all blocks at all time locations, we can conclude that with probability  $1 - \frac{WD}{|B|} \cdot D2e^{-2|B|(\beta-p)}$ , the noise absorbed in a block is less than  $|\beta|B$  for the entire computation.

Let  $X_t$  denote the support size of the error over  $B_i$  at time  $t$ . Using Claim 6.2, we can bound the total amount of error absorbed by a block until time  $t$  as follows:

$$X_t \leq \nu \cdot (X_{t-1} + \beta|B|) \leq \nu(\gamma + \beta)|B| \leq \gamma|B|$$

□

**Claim 6.5.** *The total depth of the circuit is  $O(D) + O(\log^c |B|)$ .*

*Proof.* The gate for encoding  $|B|$ -length blocks in  $C_g$  is a Clifford gate and can therefore be computed in  $O(\log |B|)$  depth. The encoding of the magic/bell states is done by first computing them in the logical space (un-encoded qubits) and then encode them using the encoder. Hence, the fault-tolerant version of both initializing ancillaries and magic states/bell states costs  $O((\log |B|) \cdot \log^c(|B| \log |B|))$ <sup>1</sup> depth [AB99]. Backing into  $C_g$  from  $C_{ft}$  by decoding the concatenation code takes exactly as long as the encoding, namely  $O((\log |B|) \cdot \log^c(|B| \log |B|))$ .

Then, using the bell measurements, any of the logical gates takes  $O(1)$  depth. Since we only perform a single round of error correction, the remaining computation until the last decoding stage takes at most constant time of the original depth. Finally, we pay  $O(\log |B|)$  for complete decoding. Summing all, we get:

$$\begin{aligned} &O(\log |B| \cdot \log^c(|B| \log |B|)) + O(D) + O(\log |B|) \\ &= O(D) + O(\log^c |B|) \end{aligned}$$

□

<sup>1</sup>The width of the original circuit is  $|B|^2$  so the number of locations is  $|B|^2 \cdot \log |B|$

Assuming that  $W$  is polynomial in  $D$ , taking the block length to be  $|B| = \log((W \cdot D)^c)$ , as shown in Claim 6.4, results in a linear fault tolerance construction with a success probability of  $1 - \frac{1}{\log^{c^2}(W \cdot D)}$ . This means that the fault tolerance version of circuits in  $\mathbf{QNC}_1$  has a logarithmic depth. Additionally, using the construction in [Aha+96] produces a polynomial fault tolerance circuit in the reversible gates setting. [COMMENT] We missed the fact that it requires non trivial classical computation to compute what gate should be applied after the gate teleportation (i.e  $UPU^\dagger$ ).

## 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>.
- [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](https://arxiv.org/abs/quant-ph/9906129) [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](https://doi.org/10.22331/q-2017-04-25-8). URL: <http://dx.doi.org/10.22331/q-2017-04-25-8>.
- [PK21] Pavel Panteleev and Gleb Kalachev. *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes*. 2021. DOI: [10.48550/ARXIV.2111.03654](https://arxiv.org/abs/2111.03654). URL: <https://arxiv.org/abs/2111.03654>.
- [Din+22] Irit Dinur et al. *Good Locally Testable Codes*. 2022. DOI: [10.48550/ARXIV.2207.11929](https://arxiv.org/abs/2207.11929). URL: <https://arxiv.org/abs/2207.11929>.
- [LZ22a] Anthony Leverrier and Gilles Zémor. *Decoding quantum Tanner codes*. 2022. arXiv: [2208.05537](https://arxiv.org/abs/2208.05537) [quant-ph]. URL: <https://arxiv.org/abs/2208.05537>.
- [LZ22b] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes*. 2022. arXiv: [2202.13641](https://arxiv.org/abs/2202.13641) [quant-ph].
- [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](https://doi.org/10.22331/q-2024-05-06-1337). URL: <http://dx.doi.org/10.22331/q-2024-05-06-1337>.