On The Cost of Fault-Tolerazing.

Michael Ben-Or   David Ponarovsky

November 7, 2024

Abstract

dddd

1 Todo:

1. Move to encoding each qubit by logarithmic width (instead of chanks) 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.

2 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 $x, y \in \{\bar{0}, \bar{1}\}$.

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

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 afterwords encode R_3 again into a good quantum code. Denote by τ the time required for decoding R_3 back, at time $t - \tau$ start to decode R_3. Eventually at time time t compute again the transversal Toffoli, by Equation (1) we gets the desired.

By similar arguments exhibited at Claim 5.3 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.

2.1 Another Idea, $z \cdot z'$ cann't contribute too mach.

Clearly we have that $|z{\cdot}z'| \leq |z|, |z'|$ therefore we have that $\mathbf{Pr}_{z,z' \in C_Z^\perp}[|z \cdot z'| \geq t] \leq \mathbf{Pr}_{z \in C_Z^\perp}[|z| \geq t]$. 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:

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

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 $_v$ 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:

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

Thus if $\mu - \gamma \geq O(1)$ (from Claim 5.2) then with high probability the Toffoli is computed up to reducible error.

3 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 Φ_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 Φ_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.

4 The Noise Model

5 Fault Tolerance (With Resets gates) at Linear Depth.

Claim 5.1. *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* $\max\{O(D), O(\log(WD))\}$.

5.1 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 5.2 (From [LZ22a]). *Assuming that an error $|e| \leq \gamma n$, i.e e is supported on less than γn bits, then a single correction round reduce e to an error e' such that $|e'| < \nu|e|$.*

Claim 5.3. *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 $1 - \frac{1}{poly(n)}$. Denote by E_i and D_i the encoder and decoder at the ith level of the concatenation construction. Consider the decoder under $\mathcal{N}$ action: $P_2 D_1 P_2 D_2, .., P_{i-1} D_i P_i$, by the fault-tolerance construction, a logical error at the ith 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 $p + p^2 + p^4 + .. < 2p$. 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:

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

Remark 5.1. *In our construction, we use the concatenation code to encode blocks of length* $\log(n)$*. Therefore, any* $poly(n)$ *in the above should be replaced by* $\log(n)$*. However, this does not affect anything since the inequality does not depend on* n*.*

□

Claim 5.4. *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* γn*.*

Proof. Consider the ith 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 5.2, 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 5.5. *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 $O((\log |B|) \cdot \log^c(|B| \log |B|))$ [1] 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:

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

□

Assuming that W is polynomial in D, taking the block length to be $|B| = \log((W \cdot D)^c)$, as shown in Claim 5.4, 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 $UPU^\dagger$).

[1] The width of the original circuit is $|B|^2$ so the number of locations is $|B|^2 \cdot \log |B|$

References

[Aha+96] D. Aharonov et al. *Limitations of Noisy Reversible Computation.* 1996. arXiv: quant-ph/9611028 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/9611028.

[AB99] Dorit Aharonov and Michael Ben-Or. *Fault-Tolerant Quantum Computation With Constant Error Rate.* 1999. arXiv: quant-ph/9906129 [quant-ph].

[PK21] Pavel Panteleev and Gleb Kalachev. *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes.* 2021. DOI: 10.48550/ARXIV.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. URL: https://arxiv.org/abs/2207.11929.

[LZ22a] Anthony Leverrier and Gilles Zémor. *Decoding quantum Tanner codes.* 2022. arXiv: 2208.05537 [quant-ph]. URL: https://arxiv.org/abs/2208.05537.

[LZ22b] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes.* 2022. arXiv: 2202.13641 [quant-ph].