

QNC₁ \subset noisy-BQP

Michael Benor David Ponomarevsky

September 18, 2024

1 Notations.

C_g - good qLDPC, C_{ft} - concatenation code (ft stands for fault tolerance). For a code C_g we use Φ_g, E_g, D_g to denote the channel maps circuits into the circuits compute in the code space, the encoder, and the decoder. We use Φ_U to denote the 'Bell'-state storing the gate U .

2 The Noise Model

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

Claim 3.1. *There is $p_{th} \in (0, 1)$ such that if $p < p_{th}$ then any quantum circuit C with depth D and width W can be computed by p -noisy, resets allowed, circuit C' , with a depth at most $\max\{D, \log(WD)\}$.*

3.1 Initializing Magic for Teleportation gates and encodes ancillaries.

The Protocol:

1. Initializing zeros. Divide the qubits into $|B|$ -size blocks. Encodes each block in C_g via $D_{ft}\Phi_{ft}[E_g] |0^{|B|}\rangle$.
2. Initializing Magic for Teleportation gates encoded in C_g via $D_{ft}\Phi_{ft}[E_g] |\Phi_U\rangle$ for each gate U in the original circuit.
3. Each gate is replaced by gate teleportation.
4. At any time tick, any block runs a single round of error reduction.

Claim 3.2. *Assume that an error $|e| = \gamma n$, i.e e is supported on less than γn bits, then a single correction round reduce e into an error e' such $|e'| < \nu|e|$.*

Definition 3.1. *We will say that a CSS code C is monotonic if for any two codewords $X_1, X_2 \in C_X/C_Z^\perp$ such that $X_1 = \sum_i g_i^{(1)}, X_2 = \sum_i g_i^{(2)}$ and $\{g^{(1)}\} \cap \{g^{(2)}\} = \emptyset$ it holds that:*

$$|X_1 + X_2| > \frac{3}{2} (|X_1| + |X_2|)$$

For example, the Toric code is monotonic. In addition it's straightforwardly to see that concatenation of two monotonic codes yield monotonic code.

Claim 3.3. *The gate $D_{ft}\Phi_{ft}[E_g]$ initializes states encoded in C_g subject to p -noise channel.*

Proof. Clearly $\Phi_{ft}[E_g]$ success, with high probability, let's say $1 - \frac{1}{\text{poly}(n)}$, to encode in to $C_{ft} \circ C_g$. Denote by E_i, D_i the encoder and the decoder at the i th level of the concatenation construction. Recall that by definition $D_i E_i = I$, or in other words $D_i = E_i^\dagger$, Hence for any paulis P_1, P_2, \dots, P_l such P_i 's can be corrected by E_i, D_i , and any two quantum states we have the following:

$$(D_1 P_2 D_2, \dots, P_{i-1} D_i P_i)^\dagger = P_i \underbrace{E_i P_{i-1} E_{i-1}, \dots, P_1 E_1}_{\star}$$

And notice that \star is with probability $1 - \frac{1}{\text{poly}(n)}$ equals to $E_i E_{i-1} \dots E_1 = E$. Hence $\mathcal{N}(D)$ equals to $(PE)^\dagger = PD$.

$$\langle \psi' | P_i E_i P_{i-1} E_{i-1}, \dots, P_1 E_1 | \psi \rangle = \langle \psi' | P_i D_i P_{i-1} D_{i-1}, \dots, P_1 D_1 | \psi \rangle$$

Thus for any pauli-channel $\mathcal{N} : L(H) \rightarrow L(H)$, and ψ' which is a codeword we get:

$$\begin{aligned} \langle \psi' | \mathcal{N}(D) | \psi \rangle &= \sum_{P_1, P_2, \dots, P_i \in \mathcal{P}} \Pr[P_1, P_2, \dots, P_i] \langle \psi' | P_i D_i P_{i-1} D_{i-1}, \dots, P_1 D_1 | \psi \rangle \\ &= \sum_{P_1, P_2, \dots, P_i \in \mathcal{P}^*} \Pr[P_1, P_2, \dots, P_i] \langle \psi' | P_i E_i P_{i-1} E_{i-1}, \dots, P_1 E_1 | \psi \rangle \pm O\left(\frac{1}{\text{poly}(n)}\right) \\ &= \sum_{P_1, P_2, \dots, P_i \in \mathcal{P}^*} \Pr[P_1, P_2, \dots, P_i] \langle \psi' | P_i E | \psi \rangle \pm O\left(\frac{1}{\text{poly}(n)}\right) \\ &\leq \sum_{P_i \in \mathcal{P}} \Pr[P_i] \langle \psi' | P_i E | \psi \rangle \pm O\left(\frac{1}{\text{poly}(n)}\right) \\ &\leq \sum_{P_i \in \mathcal{P}^d} \Pr[P_i] \langle \psi' | P_i E | \psi \rangle \pm O(e^{-d \cdot n}) \pm O\left(\frac{1}{\text{poly}(n)}\right) \\ &\leq \sum_{P_i \in \mathcal{P}/\mathcal{P}^*} \Pr[P_j \in B_d(P_i)] \langle \psi' | P_i E | \psi \rangle \pm O(e^{-d \cdot n}) \pm O\left(\frac{1}{\text{poly}(n)}\right) \end{aligned}$$

Using the fact that the concatenation code is monotonic (Definition 3.1) we get that the probability to have physical fault P_j . \square

Claim 3.4. With probability $1 - \frac{WD}{|B|} \cdot D2e^{-2|B|(\beta-p)}$, the total amount of noise been absorb in a block, in any time t , is less than γn .

Proof. Consider the i th block, denoted by B_i . Using the Hoeffding's inequality we have that the probability that more than $\beta|B|$ bits are flipped at time t is less than $\leq 2e^{-2|B|(\beta-p)}$. Using the union bounds over all the blocks at all the different time location we get that with probability $1 - \frac{WD}{|B|} \cdot D2e^{-2|B|(\beta-p)}$. Denote by X_t the support's size of the error over B_i at time t . Now using Claim 3.2, given that $X_{t-1} \leq \gamma n$ it follows that total amount of error absorbed by a block until time t can be bounded by:

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

\square