

Final Recitation – Information Theory, Application for Quantum Fault Tolerance.

David Ponarovsky

June 25, 2025

Introduction

- ▶ Nosi circuit and noisy computation.
- ▶ Classical no-go for reversible noisy computation at logarithmic depth (and polynomial space).
- ▶ Quantum case.
- ▶ Trading (local) entropy for space.

Nosiy Circuit.



Nosiy Circuit.

Definition

p - Depolarizing Channel. The qubit depolarizing channel with parameter $p \in [0, 1]$ is the quantum channel \mathcal{D}_p defined by:

$$\mathcal{D}_p(\rho) = (1 - p)\rho + p \cdot \frac{I}{2}$$

where ρ is a single-qubit density matrix and I is the identity matrix.

Definition

p -Noisy Circuit. Given a circuit C (regardless of the model), its p -noisy version \tilde{C} is the circuit obtained by alternately taking layers from C and then passing each (qu)bit through a p -Depolarizing channel.

Classical no-go.

Claim

Let Y be a bit given by moving X through $\text{BSC}(p)$, Then there is $\gamma_p < 1$ such :

$$1 - H(Y) \leq \gamma(1 - H(X))$$

Classical no-go.

Denote by δ the parameter for which X distributed as $\sim \text{Bin}(\frac{1+\delta}{2})$.
First notice that:

$$\Pr(Y = 1) = \frac{1+\delta}{2}(1-p) + \frac{1-\delta}{2}p = \frac{1+\delta-2p\delta}{2}$$

So $Y \sim \text{Bin}(\frac{1+\delta-2p\delta}{2})$, Or $\delta \mapsto 1 - 2p\delta$.

Classical no-go.

Now expand $1 - H(X)$ to it's Taylor Series at δ gives:

$$\begin{aligned}1 - H(X) &= 1 - \frac{1}{2} \left((1 + \delta) \log \left(\frac{1 + \delta}{2} \right) + (1 - \delta) \log \left(\frac{1 - \delta}{2} \right) \right) \\&= -\frac{1}{2} \left((1 + \delta) \log \left(\frac{1 + \delta}{2} \right) + (1 - \delta) \log \left(\frac{1 - \delta}{2} \right) \right) \\&= -\frac{1}{2} \cdot (1 + \delta) \sum_{i=1}^{\infty} \frac{(-1)^{i+1} \delta^i}{i} + (1 - \delta) \sum_{i=1}^{\infty} \frac{(-1)^{i+1} (-\delta)^i}{i} \\&= -\frac{1}{2} \cdot \sum_{i=1}^{\infty} 2 \frac{\delta^{2i}}{2i} - \sum_{i=1}^{\infty} 2 \frac{\delta^{2i}}{2i - 1} \\&= \sum_{i=1}^{\infty} \frac{\delta^{2i}}{2i(2i - 1)}\end{aligned}$$

Denote the above by $K(\delta)$

Classical no-go.

Now, observes that:

$$\begin{aligned} 1 - H(Y) &= K(2p\delta) = \sum_{i=1}^{\infty} \frac{(2p\delta)^{2n}}{2n(2n-1)} \\ &\leq (1-2p)^2 K(\delta) = (1-2p)^2 (1 - H(X)) \end{aligned}$$

And notice that since $p < 1$ we have $\gamma < 1$, notice also that inequality is symmetric to $p \mapsto 1-p$, in particular the entropy is not increase if either $p = 0$ or $p = 1$.

Classical no-go.

Claim

Let $Y = (Y_1, Y_2, \dots, Y_m)$ be a bit given by moving each of $X_i \in X = (X_1, X_2, \dots, X_m)$ through $\text{BSC}(p)$. Then:

$$m - H(Y) \leq \gamma(m - H(X))$$

Classical no-go.

$$\begin{aligned} m - H(Y_1, Y_2, \dots, Y_m) &= m - \sum_i H(Y_i | Y_1, Y_2, \dots, Y_{i-1}) \\ &\leq m - \sum_i H(Y_i | X_1, X_2, \dots, X_{i-1}) \\ &\leq \sum_i 1 - H(Y_i | X_1, X_2, \dots, X_{i-1}) \\ &\leq \sum_i \gamma (1 - H(X_i | X_1, X_2, \dots, X_{i-1})) \\ &\leq \gamma \sum_i (1 - H(X_i | X_1, X_2, \dots, X_{i-1})) \\ &= \gamma (m - H(X)) \end{aligned}$$

Classical no-go.

Claim

Denote by $X = (X_1, X_2, \dots, X_m)$ and $Y = (Y_1, Y_2, \dots, Y_m)$ the input and the output distributions of reversible p -noisy computation at width m (bits) and depth d . Then, there:

$$m - H(Y) \leq \gamma^d (m - H(X))$$

In particular, for $d = \Omega(\log m)$ we have $H(Y) \rightarrow m$.

Your Title Here

Your Title Here

Claim

Let ρ_1 be a reduce density matrix of ρ Then:

$$-\text{Tr } \rho \log (\rho_1 \otimes I) = S(\rho_1)$$

Your Title Here

First consider the case in which ρ is a tensor of ρ_1 namely $\rho = \rho_1 \otimes \rho_2$. Then clearly ρ and $\log \rho_1 \otimes I$ commute. Denote by $\lambda_1, \dots, \lambda_n$ and μ_1, \dots, μ_m the eigen values of ρ_1 and ρ_2 . So the trace equals:

$$\begin{aligned} \sum \lambda_i \mu_j \log(\lambda_i \cdot 1) &= \left(\sum \mu_j \right) \left(\sum_i \lambda_i \log \lambda_i \right) \\ &= (\text{Tr } \rho_2) \sum_i \lambda_i \log \lambda_i = -S(\rho_1) \end{aligned}$$

Your Title Here

Let's use the notation $\sum_{A_k} \rho|_{A_k}$ to denote the sum over all the reduced matrices over k qubits.

Claim

Let ρ be a density matrix over n qubits then:

$$\binom{n}{k}^{-1} \sum_{A_k} I(\rho|_{A_k}) \leq \frac{k}{n} I(\rho)$$

Your Title Here

Let ρ_1 be $\rho^{\otimes k \binom{n}{k}}$ and let $\rho_2 = \left(\prod_{A_k} \rho|_{A_k} \right)^{\otimes n}$.

$$\begin{aligned} 0 \geq S(\rho_2|\rho_1) &= \text{Tr} (\rho_1 (\log \rho_1 - \log \rho_2)) = -S(\rho_1) - \text{Tr} (\rho_1 \log \rho_2) \\ &= -k \binom{n}{k} S(\rho) - \sum_{A_k} \text{Tr} (\rho_1 \log (\rho|_{A_k})^n \otimes I^n) \end{aligned}$$

Now observes that $\rho|_{A_K}^{\otimes n}$ is a reduced density matrix of ρ_1 . So we get:

$$\begin{aligned} 0 &\leq -k \binom{n}{k} S(\rho) - \sum_{A_k} n S(\rho|_{A_k}) \\ \Rightarrow \sum_{A_k} I(\rho|_{A_k}) &\leq \frac{k}{n} \binom{n}{k} I(\rho) \end{aligned}$$

Your Title Here

Claim

Let ρ be a density matrix of n qubits. Let each qubit be replaced with independent probability p by a fully mixed qubit denoted by v , to give the density matrix σ . Then $I(\sigma) \leq (1 - p) I(\rho)$.

Your Title Here

Let us write:

$$\sigma = \sum_{k=1}^n \sum_{A_k} p^{n-k} (1-p)^k \rho|_{A_k} \otimes v^{n-k}$$

By the concavity of the entropy (convexity of I), We have:

$$\begin{aligned} I(\sigma) &\leq \sum_{k=1}^n \sum_{A_k} p^{n-k} (1-p)^k [I(\rho|_{A_k}) + (n-k)I(v)] \\ &= \sum_{k=1}^n \sum_{A_k} p^{n-k} (1-p)^k I(\rho|_{A_k}) \\ &\leq \sum_{k=1}^n \sum_{A_k} p^{n-k} (1-p)^k \frac{k}{n} \binom{n}{k} I(\rho) \\ &= (1-p) I(\rho) \end{aligned}$$

Your Title Here

Zeros Distillation. Consider the unitary majority gate over 3 qubits, which on the computational basis sets the last 3rd bit to be the majority, and acts as follows:

$$M |0, 0, 1\rangle \mapsto |1, 1, 0\rangle$$

$$M |1, 1, 0\rangle \mapsto |0, 0, 1\rangle$$

And acts trivially on every other configuration.

Claim

Consider the noisy zero $\rho = (1 - \frac{p}{2}) |0\rangle \langle 0| + \frac{p}{2} |1\rangle \langle 1|$. Then:

$$\text{Tr}_{[1,2]} M \rho^3 = \left(1 - \frac{3}{4}p^2 + \frac{1}{4}p^3\right) |0\rangle \langle 0| + , ,$$

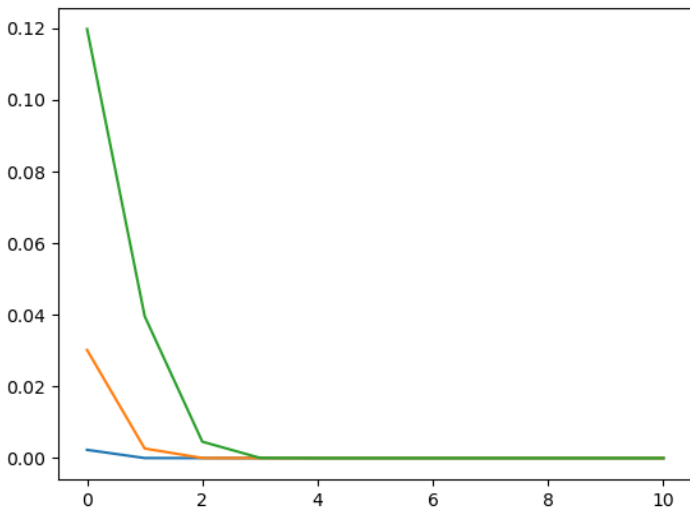
Your Title Here

$$\begin{aligned}\rho^{\otimes 3} = & \left(1 - \frac{p}{2}\right)^3 |000\rangle \langle 000| \\ & + \left(1 - \frac{p}{2}\right)^2 \frac{p}{2} (|001\rangle \langle 001| + |010\rangle \langle 010| + |100\rangle \langle 100|) \\ & + \left(1 - \frac{p}{2}\right) \left(\frac{p}{2}\right)^2 (|110\rangle \langle 110| + |101\rangle \langle 101| + |011\rangle \langle 011|) \\ & + \left(\frac{p}{2}\right)^3 |111\rangle \langle 111|\end{aligned}$$

$$\begin{aligned}M_{\rho^{\otimes 3}} = & " \\ & + \left(1 - \frac{p}{2}\right)^2 \frac{p}{2} (|110\rangle \langle 110| + ") \\ & + \left(1 - \frac{p}{2}\right) \left(\frac{p}{2}\right)^2 (|001\rangle \langle 001| + ") \\ & + "$$

$$\begin{aligned}\text{Tr}_{[1,2]} M_{\rho}^{\otimes 3} &= \left(\left(1 - \frac{p}{2}\right)^3 + 3 \left(1 - \frac{p}{2}\right)^2 \frac{p}{2} \right) |0\rangle \langle 0| + \\ &\quad + \left(3 \left(1 - \frac{p}{2}\right) \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^3 \right) |1\rangle \langle 1| \\ &= \left(1 - \frac{3}{4}p^2 + \frac{1}{4}p^3 \right) |0\rangle \langle 0| + , ,\end{aligned}$$

Your Title Here



Your Title Here

$$\begin{aligned} & \left(1 - \frac{3}{4}p^2 + \frac{1}{4}p^3\right) |0\rangle \langle 0| + , , \\ \mapsto & (1 - p) \left(1 - \frac{3}{4}p^2 + \frac{1}{4}p^3\right) |0\rangle \langle 0| + \frac{p}{2} |0\rangle \langle 0| \\ = & 1 - \frac{1}{2}p - \frac{3}{4}p^2 + p^3 - \frac{1}{4}p^4 \end{aligned}$$

Your Title Here

the probability of the thried qubit to be 1 is still less than 1. There is p_0 such that for any $p < p_0$, it follows that if each qubit has a probability less than p of being at $|1\rangle$, then after a cycle of Noise \rightarrow Majority, the probability of the third qubit being $|1\rangle$ is still less than p .

Your Title Here

Proof. After the noise round, the density matrices of each qubit:

$$\begin{aligned} &\leq (1-p)((1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|) + p\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= \left((1-p)^2 + \frac{1}{2}p\right)|0\rangle\langle 0| + \left((1-p)p + \frac{1}{2}p\right)|1\rangle\langle 1| \\ &= |0\rangle\langle 0| + (3/2p - p^2)|1\rangle\langle 1| \end{aligned}$$

And for convenience, let's bound by looking at the noisier state, where each qubit is in

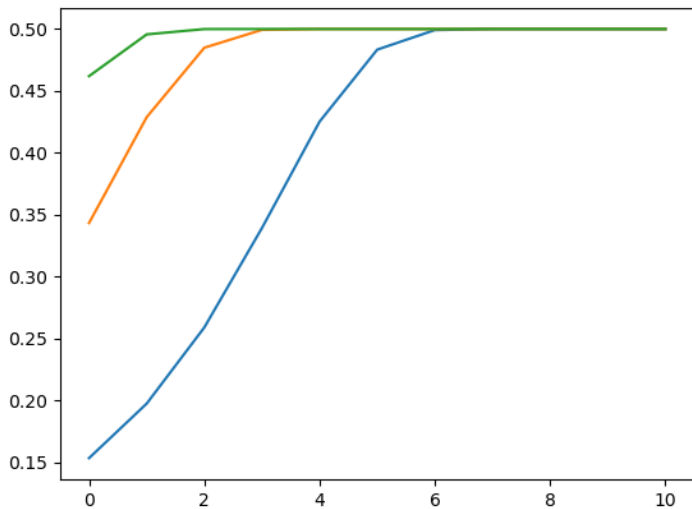
$$(1-2p)|0\rangle\langle 0| + 2p|1\rangle\langle 1|$$

Now, after applying the majority gate, the kets whose third bit is 1 are kets in $\rho^{\otimes 3}$ which absorb at least two flips. So, after tracing out the first two qubits, the coefficient of $|1\rangle\langle 1|$ would be less than:

$$(2p)^3 + 3(1-2p)(2p)^2 \leq (2p)^3 + 3(2p)^2$$

And for $p_0 = \frac{1}{6}$ we have that this probability is less than p .

Your Title Here



Your Title Here

Your Title Here