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

David Ponarovsky

June 25, 2025

Introduction

Today:

- Nosiy circuit and noisy computation.

Introduction

Today:

- Nosiy circuit and noisy computation.
- Classical no-go for reversible noisy computation at logarithmic depth (and polynomial space).

Introduction

Today:

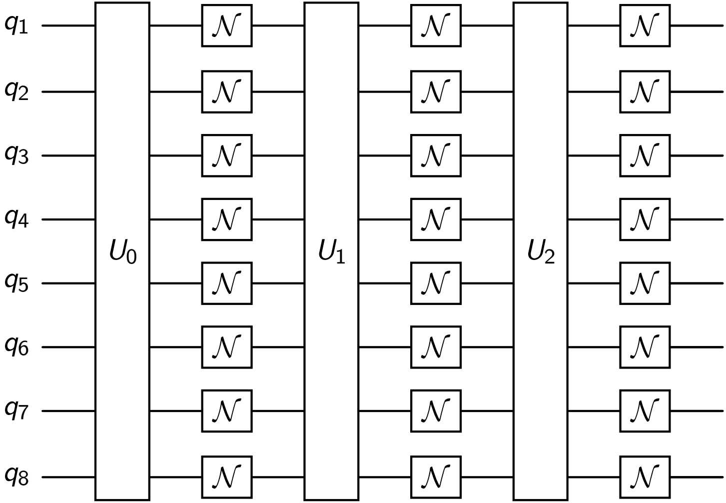
- Nosiy circuit and noisy computation.
- Classical no-go for reversible noisy computation at logarithmic depth (and polynomial space).
- Quantum case.

Introduction

Today:

- Nosiy 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.

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.

Informal:
We can't compute when subjected to noise, after a while, the bits become garbage.

Classical no-go.

Informal:

We can't compute when subjected to noise, after a while, the bits become garbage.

Claim

Denote b $X = (X_1, X_2, .., X_m)$ and $Y = (Y_1, Y_2, .., Y_m)$ the input and the output distrubtions of reversible p-noisy compuation at widith m (bits) and depth d. Then:

Classical no-go.

Informal:

We can't compute when subjected to noise, after a while, the bits become garbage.

Claim

Denote b $X = (X_1, X_2, .., X_m)$ and $Y = (Y_1, Y_2, .., Y_m)$ the input and the output distrubtions of reversible p-noisy compuation at widith m (bits) and depth d. Then:

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

Classical no-go.

Informal:

We can't compute when subjected to noise, after a while, the bits become garbage.

Claim

Denote b $X = (X_1, X_2, .., X_m)$ and $Y = (Y_1, Y_2, .., Y_m)$ the input and the output distrubtions of reversible p-noisy compuation at widith m (bits) and depth d. Then:

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

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

Classical no-go.

Claim

Let Y be a bit given by moving X trough 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:

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

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

Classical no-go.

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

$$1 - H(X) = 1 - \frac{1}{2}\left((1+\delta)\log\left(\frac{1+\delta}{2}\right) + (1-\delta)\log\left(\frac{1-\delta}{2}\right)\right)$$

Classical no-go.

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

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

Classical no-go.

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

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

Classical no-go.

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

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

Classical no-go.

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

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

Classical no-go.

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

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

Denote the above by $K(\delta)$

Classical no-go.

Now, observes that:

$$1 - H(Y) = K((1-2p)\delta) = \sum_{i=1}^{\infty} \frac{(2p\delta)^{2n}}{2n(2n-1)}$$

Classical no-go.

Now, observes that:

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

Classical no-go.

Now, observes that:

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

And notice that since $p < 1$ we have $\gamma < 1$,

Classical no-go.

Now, observes that:

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

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

Classical no-go.

Claim

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

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

Classical no-go.

Proof.

$$m - H\left(Y_1, Y_2, .., Y_m\right) = m - \sum_i H\left(Y_i \middle| Y_1, Y_2, .., Y_{i-1}\right)$$

Classical no-go.

Proof.

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

Classical no-go.

Proof.

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

Classical no-go.

Proof.

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

Classical no-go.

Proof.

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

Classical no-go.

Proof.

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

Classical no-go.

Claim

Denote b $X = (X_1, X_2, .., X_m)$ and $Y = (Y_1, Y_2, .., Y_m)$ the input and the output distrubtions of reversible p-noisy compuation at widith m (bits) and depth d. Then:

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

Classical no-go.

Claim

Denote b $X = (X_1, X_2, .., X_m)$ and $Y = (Y_1, Y_2, .., Y_m)$ the input and the output distrubtions of reversible p-noisy compuation at widith m (bits) and depth d. Then:

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

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

Quantum no-go.

Let's continue to the quantum case. From now on we will denote by $I(\rho) = \dim \rho - S(\rho)$.

Quantum no-go.

Let's continue to the quantum case. From now on we will denote by $I(\rho) = \dim \rho - S(\rho)$.For repeating the above w'll have to prove more claims.

Quantum no-go.

Claim

Let ρ_1 be a reduce density matrix of ρ Then:

$$-\mathbf{Tr}\ \rho \log\left(\rho_1 \otimes I\right) = S(\rho_1)$$

Quantum no-go.

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 $\lambda_1, ..\lambda_n$ and $\mu_1, ..\mu_m$ the eigen values of ρ_1 and ρ_2. So the trace equals:

$$\sum \lambda_i \mu_j \log(\lambda_i \cdot 1) = \left(\sum \mu_j\right) \left(\sum_i \lambda_i \log \lambda_i\right)$$

Quantum no-go.

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 $\lambda_1, ..\lambda_n$ and $\mu_1, ..\mu_m$ the eigen values of ρ_1 and ρ_2. So the trace equals:

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

Quantum no-go.

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 $\lambda_1, ..\lambda_n$ and $\mu_1, ..\mu_m$ the eigen values of ρ_1 and ρ_2. So the trace equals:

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

Then consider the case where ρ is entangle. Let's span ρ over base at the form $\{\rho_1 \otimes \rho_2^i\}$ We get:

$$\begin{aligned} \mathbf{Tr}\ \rho \log(\rho_1 \otimes I) &= \mathbf{Tr}\ \sum_i a_i \rho_1 \otimes \rho_2^i \log(\rho_1 \otimes I) \\ &= -\sum_i a_i S(\rho_1) = -S(\rho_1) \end{aligned}$$

Quantum no-go.

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:

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

Quantum no-go.

Proof

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

$$0 \leq S(\rho_2||\rho_1) = \mathbf{Tr}\ \left(\rho_1\left(\log\rho_1 - \log\rho_2\right)\right) = -S(\rho_1) - \mathbf{Tr}\ \left(\rho_1 \log\rho_2\right)$$

Quantum no-go.

Proof

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

$$0 \leq S(\rho_2||\rho_1) = \mathbf{Tr}\ \left(\rho_1 \left(\log \rho_1 - \log \rho_2\right)\right) = -S(\rho_1) - \mathbf{Tr}\ \left(\rho_1 \log \rho_2\right)$$
$$= -k\binom{n}{k} S(\rho) - \sum_{A_k} \mathbf{Tr}\ \left(\rho_1 \log \left(\rho|_{A_k}\right)^n \otimes I^n\right)$$

Quantum no-go.

Proof

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

$$0 \leq S(\rho_2||\rho_1) = \mathbf{Tr}\ \left(\rho_1 \left(\log \rho_1 - \log \rho_2\right)\right) = -S(\rho_1) - \mathbf{Tr}\ \left(\rho_1 \log \rho_2\right)$$
$$= -k\binom{n}{k} S(\rho) - \sum_{A_k} \mathbf{Tr}\ \left(\rho_1 \log \left(\rho|_{A_k}\right)^n \otimes I^n\right)$$

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

$$0$$

$$\Rightarrow$$

Quantum no-go.

Proof

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

$$0 \leq S(\rho_2||\rho_1) = \mathbf{Tr}\ \left(\rho_1 \left(\log \rho_1 - \log \rho_2\right)\right) = -S(\rho_1) - \mathbf{Tr}\ \left(\rho_1 \log \rho_2\right)$$
$$= -k\binom{n}{k} S(\rho) - \sum_{A_k} \mathbf{Tr}\ \left(\rho_1 \log \left(\rho|_{A_k}\right)^n \otimes I^n\right)$$

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

$$0 \leq -k\binom{n}{k} S(\rho) + \sum_{A_k} nS\left(\rho|_{A_k}\right)$$

$$\Rightarrow$$

Quantum no-go.

Proof

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

$$0 \leq S(\rho_2||\rho_1) = \mathbf{Tr}\ (\rho_1 (\log \rho_1 - \log \rho_2)) = -S(\rho_1) - \mathbf{Tr}\ (\rho_1 \log \rho_2)$$
$$= -k\binom{n}{k} S(\rho) - \sum_{A_k} \mathbf{Tr}\ \left(\rho_1 \log \left(\rho|_{A_k}\right)^n \otimes I^n\right)$$

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

$$0 \leq -k\binom{n}{k} S(\rho) + \sum_{A_k} nS\left(\rho|_{A_k}\right)$$
$$\Rightarrow \sum_{A_k} I\left(\rho|_{A_k}\right) \leq \frac{k}{n}\binom{n}{k} I\left(\rho\right)$$

Quantum no-go.

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 υ, to give the density matrix σ. Then $I(\sigma) \leq (1-p)\, I(\rho)$.

Quantum no-go.

Let us write:

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

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

$$I(\sigma)$$

Quantum no-go.

Let us write:

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

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

$$I(\sigma) \leq \sum_{k=1}^{n} \sum_{A_k} p^{n-k} (1-p)^k \left[I(\rho|_{A_k}) + (n-k) I(\upsilon) \right]$$

Quantum no-go.

Let us write:

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

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

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

Quantum no-go.

Let us write:

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

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

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

Quantum no-go.

Let us write:

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

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

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

Entropy-Space tradeoff.

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.

Entropy-Space tradeoff.

Claim

There is a 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.

Entropy-Space tradeoff.

Proof.

After the noise round, the density matrices of each qubit[1]:

$$\leq (1-p)\left((1-p)\left|0\right\rangle\left\langle 0\right| + p\left|1\right\rangle\left\langle 1\right|\right) + p\frac{1}{2}\left(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|\right)$$

[1] The inequality refers to the $\left|1\right\rangle\left\langle 1\right|$ coefficient.

Entropy-Space tradeoff.

Proof.

After the noise round, the density matrices of each qubit[1]:

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

[1] The inequality refers to the $\left|1\right\rangle\left\langle 1\right|$ coefficient.

Entropy-Space tradeoff.

Proof.

After the noise round, the density matrices of each qubit[1]:

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

[1]The inequality refers to the $\left|1\right\rangle\left\langle 1\right|$ coefficient.

Entropy-Space tradeoff.

Proof.

After the noise round, the density matrices of each qubit[1]:

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

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

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

[1] The inequality refers to the $\left|1\right\rangle\left\langle 1\right|$ coefficient.

Entropy-Space tradeoff.

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

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

Now, after applying the majority gate, the kets whose third bit is 1 are kets in $\rho^{\otimes 3}$ that absorb at least two flips.

Entropy-Space tradeoff.

And for convenience, let's bound it by looking at the following 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 $\rho^{\otimes 3}$ that absorb at least two flips. Thus, after tracing out the first two qubits, the coefficient of $|1\rangle \langle 1|$ would be less than:

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

Entropy-Space tradeoff.

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

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

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

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

Entropy-Space tradeoff.

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

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

Now, after applying the majority gate, the kets whose third bit is 1 are kets in $\rho^{\otimes 3}$ that absorb at least two flips. Thus, after tracing out the first two qubits, the coefficient of $\left|1\right\rangle\left\langle 1\right|$ 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.

The End.

June 25, 2025