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

David Ponarovsky

June 21, 2025

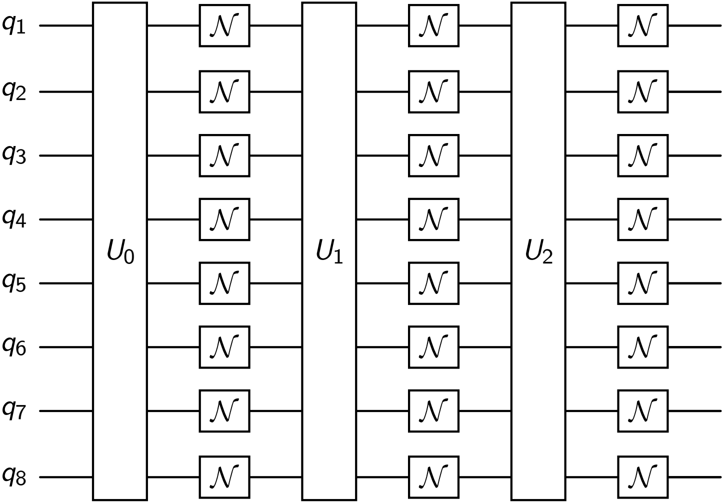
Introduction

- Brief overview of the topic
- Importance and relevance
- Objectives of the presentation

Key Points

- Main point 1
- Main point 2
- Main point 3

Your Title Here



Your Title Here

Claim

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

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

Your Title Here

Denote by δ the parameter for which X distributed as $\sim \mathrm{Bin}(\frac{1+\delta}{2})$.
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 $Y \sim \mathrm{Bin}(\frac{1-\delta(1-2p)}{2})$, Or $\delta \mapsto 1-2p\delta$.

Your Title Here

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 $K(\delta)$

Your Title Here

Now, observes that:

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

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 $p = 1$.

Your Title Here

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:

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

Your Title Here

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

Your Title Here

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, there:

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

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

Your Title Here

Your Title Here

Claim

Let ρ_1 be a reduce density matrix of ρ Then:

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

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

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

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 $\rho_2 = \left(\prod_{A_k} \rho|_{A_k}\right)^{\otimes n}$.

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

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

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

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

Your Title Here

Let us write:

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

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

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

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:

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

And acts trivially on every other configuration.

Claim

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

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

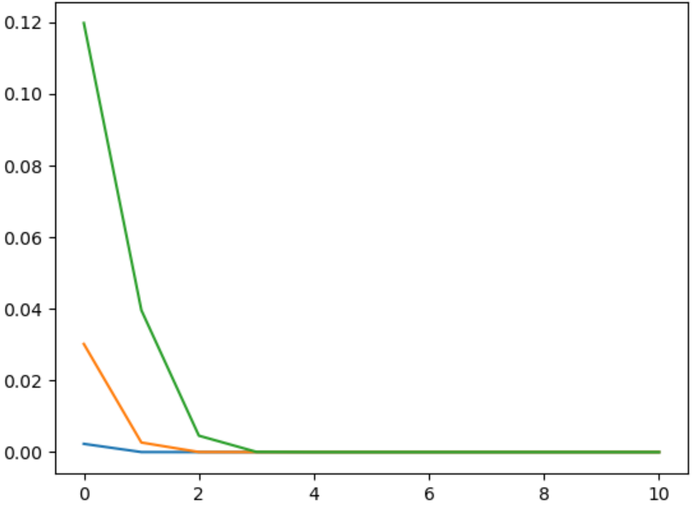
Your Title Here

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

Your Title Here

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

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:

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

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

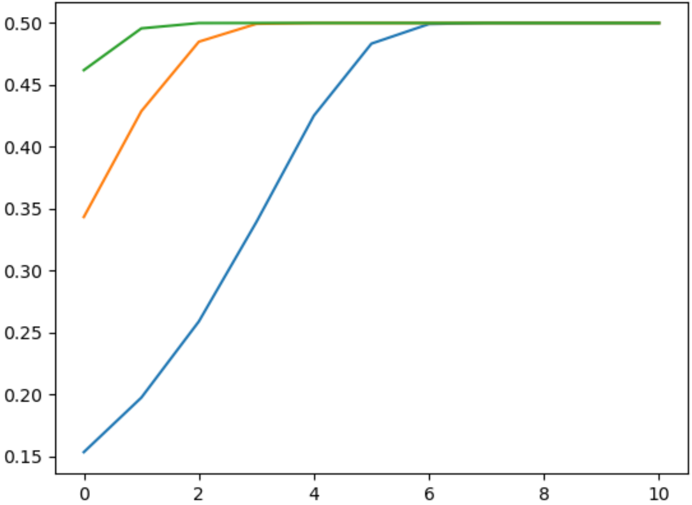
$$(1-2p)\left|0\right\rangle\left\langle 0\right| + 2p\left|1\right\rangle\left\langle 1\right|$$

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

Your Title Here



Your Title Here

Your Title Here