

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

David Ponarovsky

June 20, 2025

Key Points

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

Your Title Here

Claim

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

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

Your Title Here

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 $Y \sim \text{Bin}(\frac{1+\delta(1-2p)}{2})$, 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:

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

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 $p = 1$.

Your Title Here

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:

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

Your Title Here

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

Your Title Here

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:

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