Quantum Fano's inequality

Chen Li[1]

[1] *Department of Physics, University of California at San Diego, La Jolla, CA 92093*

Fano's inequality, being used in the classic information theory, could be transplanted to quantum field to study the noise caused by quantum operations. All proof is based on [1] and [2]

INTRODUCTION

Fano's inequality is a very important theorem that is used in the classic information theory to explore the bound of conditional entropy when making estimations for a certain random variable. Similarly, in the quantum computing, a new concept Entropy exchange, a measurement of how much noise caused when applying a quantum operation to a quantum state, could be an analogy to the conditional entropy in the classic information theory and could be used to derive the quantum Fano's inequality.

CLASSIC FANO'S INEQUALITY

Let's start with the Fano's inequality in the classic information theory. A markov chain $X \to Y \to \hat{X}$ with a random variable X and the estimation $\hat{X}$ we get out of observation Y. The easiest way to think this markov chain is the communication channel such that Y equal to the noise plus the X and $\hat{X}$ is the estimation made based on Y. Thus, the best case is that $H(X|\hat{X}) = 0$ which means that our estimation completely recover the original X with no errors, but this is basically impossible in most other cases, and consequently we are interested in how much information is lost through the channel, in other words $H(X|\hat{X})$, how much uncertainty X still has given the estimation $\hat{X}$.

Because it's not ideal, making errors is inevitable and we define $P_e = P(\hat{X} \neq X)$ and a new random variable Z [2].

$$Z = \begin{cases} 1, \text{if} \quad \hat{X} \neq X & \text{w.p} \;\; Pe \\ 0, \text{if} \quad \hat{X} = X & \text{w.p} \;\; 1 - Pe \end{cases}$$

Then we could start deriving the conditional entropy $H(X|\hat{X})$ [2]

$$\begin{aligned} H(X|\hat{X}) &= H(X|\hat{X}) + H(Z|X, \hat{X}) \\ &= H(X, Z|\hat{X}) \\ &= H(Z|X) + H(X|Z, \hat{X}) \\ &\leq H(Z) + P_e H(X|\hat{X}, Z = 1) \\ &\quad + (1 - P_e) H(X|\hat{X}, Z = 0) \\ &\leq H(P_e) + P_e log(|X| - 1) \end{aligned}$$

To understand this inequality more easily, we can extend it a little bit:

$$H(X|\hat{X}) \leq H(P_e) + P_e log(|X| - 1) + (1 - P_e) log(1)$$

Then the information lost in the channel is, intuitively, the amount of information that P_error itself has, plus the amount of information of the correct symbol(outcomes of random variable), then plus the amount of information of all other symbols except the correct one. Because we are trying find the maximum, the information could be maximized when every symbol is equal probable and this is how cardinality $|X|$ comes from.

SOME TRANSFORMATIONS

The equation given in the previous part is in term of $H(X|\hat{X})$, however, people are more interested in $H(X|Y)$ because Y is what we actually observed. According to the data processing Inequality [2]:

$$I(X; \hat{X}) \leq I(X; Y)$$

Then we can expand the inequality:

$$\begin{gathered} H(X) - H(X|\hat{X}) \leq H(X) - H(X|Y) \\ H(X|Y) \geq H(X|\hat{X}) \end{gathered}$$

Thus the fano's inequality becomes:

$$H(X|Y) \leq H(P_e) + P_e log(|X| - 1)$$

Because P_e is as Bernoulli random variable and due to its concavity, the maximum entropy is equal to 1 when $P_e = \frac{1}{2}$ [2]:

$$\begin{gathered} H(X|Y) \leq 1 + P_e log(|X| - 1) \\ P_e \geq \frac{H(X|Y) - 1}{log(|X| - 1)} \end{gathered}$$

Now this form is very useful and it gives us an lower bound on the error probability in term of conditional entropy.

ENTROPY EXCHANGE

The same idea from the classic conditional entropy $H(X|\hat{X})$ could be used to explain the quantum entropy exchange: $S(\rho, \varepsilon)$ is a measurement the information lost when the operation ε applied to the state ρ. The operation ε with operation elements E_i could be represented by defining an unitary operator [1]:

$$U|\psi\rangle|0\rangle = \sum_i E_i|\psi\rangle|1\rangle$$

Then

$$\rho^{E'} = \sum_{i,j} tr(E_i \rho E_j^\dagger)|i\rangle|j\rangle$$

From this, we successfully convert an operation with element E_i applying on state ρ into a new-defined matrix W with elements $tr(E_i \rho E_j^\dagger)$ and therefore when calculate the entropy exchange, we simply evaluate the $-tr(WlogW)$ [1].

$$S(\rho, \varepsilon) = S(R', Q') = S(W) = -tr(WlogW)$$

This form with W is termed canonical form and when dealing with this form, some properties could be directly borrowed from classic information theory: when applying the operation ε on d-dimensional, the best case we can get is $S(\frac{I}{d}, \varepsilon) = 0$ which is similar to $H(X|\hat{X}) = 0$, conveying that no information is lost during this operation [1].

QUANTUM FANO'S INEQUALITY

The same intuition from classic Fano's inequality could be used here to understand quantum errors: the noise generated in the operation to make entangled RQ to be mixed, which is analogy to the noise destroying the signal in the channel, then, the fidelity, which is similar to P_e that will get worse when noise is greateer, would be a problem at the final state R'Q'.

So, Quantum Fano's inequality is very similar idea and we just substitute P_e with fidelity and conditional entropy with entropy exchange [1]:

$$S(\rho, \varepsilon) \leq H(F(\rho, \varepsilon)) + (1 - F(\rho, \varepsilon))log(d^2 - 1)$$

I will go throug the proof very briefly and it starts from the result from entropy measurement [1]:

$$S(\rho, \varepsilon) \leq H(p_1, p_2.....p_{d^2})$$

Then we need to use grouping property from classic information theory to expand RHS:

$$\begin{aligned} H(p_1, p_2.....p_{d^2}) &= H(p_1) - \sum_{i=2}^{d^2} p_i log p_i \\ &= H(p_1) - (1 - p_1) \sum_{i=2}^{d^2} \frac{p_i}{1 - p_1} log \frac{p_i}{1 - p_1} \\ &= H(p_1) + (1 - p_1) H(\frac{p_2}{1 - p_1}, ... \frac{p_d^2}{1 - p_1}) \end{aligned}$$

Using this sauce we get the inequality:

$$\begin{aligned} S(\rho, \varepsilon) &\leq H(p_1) + (1 - p_1) H(\frac{p_2}{1 - p_1}, ... \frac{p_d^2}{1 - p_1}) \\ &\leq H(p_1) + (1 - p_1) log(d^2) \end{aligned}$$

Then we substitute p_1 with my fidelity $F(\rho, \varepsilon)$ [1]:

$$S(\rho, \varepsilon) \leq H(F(\rho, \varepsilon)) + (1 - F(\rho, \varepsilon))log(d^2 - 1)$$

It is worth noting that the cardinality becomes d^2 because we are dealing with two dimensional. This gives an upper bound of the information lost in the quantum channel and the probability that the one state would be identified as the other. Consequently, this ineuqlity could be used as a good reference when studying how to transmit the entangled states through the noisy quantum channel.

SOME QUESTIONS

People proved that entropy exchange is also a concave function respect to ε and it should have a maximum numeric value. We then could weaken the inequality by writing the $H(F(\rho, \varepsilon))$ as its maximum. As we can see, we could transform the equations in the classic fano's inequality to form a lower bound on the probability of error. This makes me wondering that if we could do the same thing for the quantum fano's inequality to form a lower bound for fidelity $F(\rho, \varepsilon)$, in other words, a lower bound of how close these quantum states are between the source Q and final Q'.

BIBLIOGRAPHY

[1] Michael A. Nielsen & Isaac L. Chuang, "Quantum Computation and Quantum Information," Cambirdge University Press(2010).

[2] Thomas M. Cover & Joy A. Thomas, "Elements of Information Theory," John Wiley & Sons, Inc., Hoboken, NJ(2006).