Quantum Information
Week 5

Instructed by *Mile Gu*

Li Chenxing 李辰星 JK30 2013012479

1 Shannon Entropy

In this section, we consider the entropy on z basis. Consider the density matrix ρ of the classical coin.

$$\rho = c_0|0\rangle\langle 0| + c_1|1\rangle\langle 1|.$$

Then the entropy of ρ is

$$S(\rho) = -c_0 \log c_0 - c_1 \log c_1.$$

Generally, we can define the entropy of the density matrix

$$S(\rho) = -\sum_{\lambda} \lambda \log(\lambda) = -\mathrm{Tr}[\rho \log \rho].$$

2 Mutual entropy

We use $H(X)$ to denote the entropy of random variable X, and $H(X|Y)$ to denote the condition entropy of X given Y. The definition of condition entropy will be proposed later on.

Suppose random variable X, Y are independent, then we can not get more information about X even if we are given Y. Which means

$$H(X) - H(X|Y) = 0.$$

If we are given $Y = y$, then the entropy of X will be $H(X|Y = y)$.

$$H(X|Y = y) = -\sum_{i} \Pr[x_i|Y = y] \log(\Pr[x_i|Y = y]).$$

The formal definition of condition entropy is

$$H(X|Y) = \sum_{y} \Pr[Y = y] \cdot H(X|Y = y) = -\sum_{x,y} \Pr[X = x, Y = y] \log(\Pr[X = x|Y = y]).$$

Also we have

$$
\begin{aligned}
& -\sum_{x,y} \Pr[X=x,Y=y]\log(\Pr[X=x|Y=y]) \\
=& -\sum_{x,y} \Pr[X=x,Y=y]\left(\log(\Pr[X=x,Y=y]) - \log(\Pr[Y=y])\right) \\
=& -\sum_{x,y} \Pr[X=x,Y=y]\log(\Pr[X=x,Y=y]) + \sum_{x,y} \Pr[X=x,Y=y]\log(\Pr[Y=y]) \\
=& -\sum_{x,y} \Pr[X=x,Y=y]\log(\Pr[X=x,Y=y]) + \sum_{y} \Pr[Y=y]\log(\Pr[Y=y]) \\
=& H(X,Y) - H(Y)
\end{aligned}
$$

The mutual entropy is defined as

$$I(X,Y) = H(X) - H(X|Y) = H(X) + H(Y) - H(X,Y).$$

3 Holevo's Theorem

A qubit has entropy at most 1. This means you can not communicate more than 1 bit information with 1 qubit.

If Alice want to transfer with 2 qubit, she encode such that

00	01	10	11
$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$

Bob can not distinguish non-othorganal. So such transfermation cannot success.

But if Alice and Bob obtain a pair of entangle qubits $|\psi\rangle_{AB} = |00\rangle + |11\rangle$. Alice can encode the 2 bits by appling measurement $I, \sigma_x, \sigma_z, \sigma_x\sigma_z$ and transfer this qubit to Bob. When bob get qubits, he can perform opreation C-NOT, and measure the first qubit in σ_x basis and the second qubit in σ_z basis.

4 A paradox

For entangle qubit, we may have

$$H(X,Y) = 0, H(X) = 1, H(Y) = 1.$$

In this way

$$H(X|Y) = H(X,Y) - H(Y) = -1.$$