Quantum and Classical Information

What is the relationship between classical and quantum information?

Qubits are more complicated that bits

Probabilistic bit: $P(0) = p \quad P(1) = 1-p$

Qubit: $\rho = \frac{1}{2}\left(\mathbb{1} + \langle\sigma_x\rangle\sigma_x + \langle\sigma_y\rangle\sigma_y + \langle\sigma_z\rangle\sigma_z\right)$

$= \frac{1}{2}\left(\mathbb{1} + (2p_x-1)\sigma_x + (2p_y-1)\sigma_y + (2p_z-1)\sigma_z\right)$

$(2p_x-1)^2 + (2p_y-1)^2 + (2p_z-1)^2 \leq 1$

This would suggest that 1 qubit = 3 bits

But even though 3 bits can go in, can we read them out?

How many bits can one store in a qubit?

At least 1: $0 \to |0\rangle \quad 1 \to |1\rangle$

For an upper bound, we need to define some tools

Tool 1: Von Neumann and Shannon entropies

These are defined respectively for density matrices and probability distributions

$$S(\rho) \qquad H[P(x)]$$

The former describes a quantum system, A, and the latter describes a random variable, X, so we sometimes write

$$S(A) \qquad H(X)$$

When do they describe the same thing?

The quantum system A measured with a specific basis is a random variable X

$$X : x \in \{x_1, \ldots, x_d\} \qquad P_j = \langle x_j | \rho | x_j \rangle$$

If this is the eigenbasis of the density matrix

$$S(A) = H(X)$$

Tool 2: (Strong) subadditivity

There are many useful properties of Shannon and Von Neumann entropies that are good to know and understand (see chapter 11 of N+C)

One is subadditivity (N+C 11.3.4)

$$H(XY) \leq H(X) + H(Y)$$

$$S(AB) \leq S(A) + S(B)$$

The other is strong subadditivity (N+C 11.4)

$$H(XYZ) + H(Y) \leq H(XY) + H(YZ)$$

$$S(ABC) + S(B) \leq S(AB) + S(BC)$$

To apply these, let us first define the quantum mutual information in analogy with the classical one

$$I(A;B) = S(A) + S(B) - S(AB)$$

From subadditivity we then find that the mutual information is always non-negative

$$S(AB) \leq S(A) + S(B), \qquad S(A) + S(B) - S(AB) \geq 0$$

$$\therefore\ I(A;B) \geq 0$$

Strong subadditivity allows us to show that the MI does not increase when subsystems are discarded

$$S(ABC) + S(B) \leq S(AB) + S(BC)$$

$$S(BC) - S(ABC) \geq S(B) - S(AB)$$

$$S(A) + S(BC) - S(ABC) \geq S(A) + S(B) - S(AB)$$

$$\therefore\quad I(A;BC) \geq I(A;B)$$

Both as we'd want for the MI

Tool 3: Unitary Invariance

The entropy is defined using the eigenvalues of the density matrix

The action of a unitary on a density matrix does not change its eigenvalues

So $S(\rho) = S(U\rho U^\dagger)$

Similarly, local unitaries do not change the mutual information

$$I(A;B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$
$$= S(U_A \rho_A U_A^\dagger) + S(U_B \rho_B U_B^\dagger) - S(U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger)$$

Tool 4: Entropy of a tensor products and pure states

It is fairly straightforward to show

$S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$, $S(|\psi\rangle\langle\psi|) = 0$

Holevo Bound

Suppose that Alice has the outcome of a random variable

$$\rho_A = \sum_j P_j |x_j\rangle\langle x_j| \qquad \langle x_i|x_j\rangle = \delta_{i,j}$$

She wants to store it in a qubit and send it to Bob, so she prepares a different qubit state $|\psi_j\rangle$ for each outcome $|x_j\rangle$

$$U_{AQ}: \rho_A \otimes |0\rangle\langle 0| \rightarrow \rho_{AQ} = \sum_j P_j |x_j\rangle\langle x_j| \otimes |\psi_j\rangle\langle\psi_j|$$

If the random variable had two outcomes, she could use orthogonal states $|\psi_1\rangle = |0\rangle$, $|\psi_2\rangle = |1\rangle$

Bob could then measure the qubit in the Z basis, and determine x_j

So we can store at least one bit in a qubit

What about a random variable with >2 outcomes?

The states $|\psi_j\rangle$ can no longer be mutually orthononal

Can Bob still distinguish them by measurement?

Most general kind of measurement he could do is to take an extra quantum system, M, and measure the joint system QM in some clever basis

$$\rho_{AQM} = \sum_j p_j |x_j\rangle\langle x_j| \otimes |\psi_j\rangle\langle\psi_j| \otimes |0\rangle\langle 0|^{\otimes m}$$

$$= \sum_j p_j |x_j\rangle\langle x_j| \otimes \sum_{k,k'} c_{jk} c_{jk'}^* |\mu_k\rangle\langle\mu_{k'}|$$

$$|\psi_j\rangle \otimes |0\rangle^{\otimes m} = \sum_k c_{jk} |\mu_k\rangle \qquad \langle\mu_j|\mu_k\rangle = \delta_{ij}$$

Suppose that, to measure, he must copy the result to another system C

$$U_{QMC} : \left(|\psi_j\rangle \otimes |0\rangle^{\otimes m}\right) \otimes |0\rangle^{\otimes m+1} \to \sum_k c_{jk} |\mu_k\rangle \otimes |\mu_k\rangle$$

The state is then

$$\rho_{AQMC} = \sum_j p_j |x_j\rangle\langle x_j| \otimes \sum_{k,k'} c_{jk} c_{jk'}^* |\mu_k\rangle\langle\mu_{k'}| \otimes |\mu_k\rangle\langle\mu_{k'}|$$

First trace out A. Easy because it's diagonal

$$\rho_{QMC} = tr_A(\rho_{AQMC}) = \sum_{j,k,k'} p_j c_{jk} c_{jk'}^* |\mu_k\rangle\langle\mu_{k'}| \otimes |\mu_k\rangle\langle\mu_{k'}|$$

Now trace over QM (so ignore cases when k isn't k')

$$\rho_C = tr_{QM}(\rho_{QMC}) = \sum_{jk} p_j |c_{jk}|^2 |\mu_k\rangle\langle\mu_k|$$

This is diagonal in the basis in which it will be measured

$S(\rho_C) = H(Y)$ $\quad$ Y is random variable defined by results

$\therefore I(X;Y) = I(A;C)$ $\quad$ (since $S(A) = H(X)$)

The mutual information between A and C can therefore tell us how much classical information Bob can extract about Alice's classical results

Using strong subadditivity

$$I(A;C) \leq I(A;QMC)$$

Using unitary invariance we can calculate $I(A;QMC)$ with the state before the copy

$$\rho_{AQMC} = \left(\sum_j p_j |x_j\rangle\langle x_j| \otimes |\psi_j\rangle\langle\psi_j|\right) \otimes |0\rangle\langle 0|^{\otimes m} \otimes |0\rangle\langle 0|^{\otimes m+1}$$

Using the properties of the entropy for tensor products and pure states, M and C clearly do not contribute

$$I(A;QMC) = I(A;Q)$$

$$S(A) = H(X), \quad S(AQ) = H(X), \quad S(Q) = S(\rho_Q)$$

(unitary invariance again ↑)

$$\therefore I(A;Q) = S(\rho_Q) \therefore I(X;Y) \leq S(\rho_Q) \leq 1 \text{ b.t}$$

So Bob can determine at most one bit about Alice's random variable (the accessible information)

In general, Alice could have prepared mixed states ρ_j for the qubit instead of pure ones $|\psi_j\rangle\langle\psi_j|$

The bound would then be

$$I(X;Y) \leq S(\rho_Q) - \sum_j p_j S(\rho_j)$$

This is called the Holevo bound (N+C 12.1.1, P 5.3.3-5.4)