C2: Quantum information basics

Rob Smith

Lecture 6

7 Measurement, fidelity and entanglement

7.1 Measuring a single qubit

An important result in the field of quantum information is that *no experiment allows us to find out the state of a generic unknown single qubit.* A measurement of state $\alpha|0\rangle + \beta|1\rangle$ will either return a 1 or a 0 with probabilities $\alpha\alpha^*$ and $\beta\beta^*$ respectively. Performing repeated measurements of the same qubit will not help as the first measurement collapses the state of the qubit to either $|0\rangle$ or $|1\rangle$ and so subsequent measurements will just give the same answer.

It is, however, possible to determine the state of this system if some prior information is known about it. For example, if we know the state is either $|0\rangle$ or $|1\rangle$ then a measurement can tell us definitively which. More generally, the measurement will only be perfect if the measurement axis is parallel (or anti-parallel) to the state. So given the prior information we need to optimise the measurement we perform. For example, if we knew the state was either $|\pm\rangle$ then measuring in the z–basis ($|0\rangle$, $|1\rangle$) is not a smart thing to do – instead we should measure in the x–basis (or apply a H gate and then measure along z).

7.2 No cloning theorem

One idea to solve this measurement problem would be to copy the qubit such that we have N identical copies of the same state; if this were possible we could estimate $\alpha\alpha^*$ and $\beta\beta^*$ up to a statistical error which goes as $\sim 1/\sqrt{N}$. However, making copies of a generic quantum state is impossible - this is known as the *no-cloning theorem.* It's proof relies on the linearity of quantum mechanics and is shown by contradiction.

We want an operator U_{copy} such that

$$|A_i\rangle|\psi\rangle \xrightarrow{U_{\text{copy}}} |A_f\rangle|\psi\rangle|\psi\rangle; \tag{40}$$

note that we have created a copy of $|\psi\rangle$ and $|A\rangle$ represents the rest of the system. Applying U_{copy} to $|0\rangle$, $|1\rangle$ and the general state $\alpha|0\rangle + \beta|1\rangle$ gives

$$|A_i\rangle|0\rangle \xrightarrow{U_{\text{copy}}} |A_0\rangle|00\rangle, \tag{41}$$

$$|A_i\rangle|1\rangle \xrightarrow{U_{\text{copy}}} |A_1\rangle|11\rangle, \tag{42}$$

and

$$|A_i\rangle(\alpha|0\rangle + \beta|1\rangle) \xrightarrow{U_{\text{copy}}} \alpha|A_0\rangle|00\rangle + \beta|A_1\rangle|11\rangle, \tag{43}$$

but we can also write

$$|A_i\rangle(\alpha|0\rangle + \beta|1\rangle) \xrightarrow{U_{\text{copy}}} |A_f\rangle(\alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|00\rangle), \tag{44}$$

which (whatever we choose for $|A_0\rangle$, $A_1\rangle$ and $A_f\rangle$ cannot be made the same as Eq.(43) unless $|\alpha^2| = 1$ or 0.

7.3 State and gate fidelity

Fidelity measures how close two states are to one another, there is no unique way to do this but it is conventional to use the inner product:

$$F(\psi, \phi) = |\langle\phi|\psi\rangle|^2 = \langle\phi|\psi\rangle\langle\psi|\phi\rangle = \langle\phi|\hat{\rho}_\psi|\phi\rangle. \tag{45}$$

For example the fidelity of a (ensemble) state and the same state after a measurement would be:

$$F = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha\alpha^* & 0\\ 0 & \beta\beta^*\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = |\alpha|^2 + |\beta|^4 = 1 - 2|\alpha|^2 + 2|\alpha|^4; \tag{46}$$

we have $F = 1$ for $|\alpha|^2 = 0$ or 1 and a minimum $F = 1/2$ for $|\alpha|^2 = |\beta|^2 = 1/2$.

By extension the fidelity of a gate is defined by the fidelity of the state it does produce with the state produced by the ideal gate.

7.4 Local operations and classical communication (LOCC)

Consider the following scenario, which is usually called LOCC:

- Alice and Bob each have access to one qubit of a two–qubit system,
- they can only manipulate their own qubit,
- they can also communicate classically with one another.

If the two qubits are in a separable state then nothing interesting happens (we just have two individual single qubit systems which Alice and Bob can independently operate on without having any consequences for the other qubit). However, if the qubits are in an entangled state then this is no longer the case, we can no-longer divide the system up into portions controlled by Alice and those controlled by Bob. For example, local operations by either Alice or Bob can change the two–qubit state from one Bell state to another (e.g. applying a local NOT to either of the qubits in $|\phi^+\rangle$ changes it to $|\psi^+\rangle$). This can be used in quantum communication protocols that will be discussed later in the course. It is important to note however that *the degree of entanglement cannot be increased via LOCC*. Entanglement production requires two-qubit gates which means the two qubits must be in contact (interacting) with one another.