Quantum Computing (CST Part II)

Lecture 4: Important Concepts in Quantum Mechanics

The 'paradox' is only a conflict between reality and your feeling of what reality 'ought to be'.

Richard Feynman

Resources for this lecture

From **Nielsen and Chuang**:

- Distinguishing quantum states: **p86, p529**
- The no-cloning theorem: **p532**

What are these “important concepts”?

How much (classical) information can we get out of a quantum state?

Some “no-go” theorems.

… and why should we care?

How much (classical) information can we get out of a quantum state?

- What if we don't just want to distinguish orthogonal states?
- Important for some applications e.g., security.

Some "no-go" theorems.

- To get a physical grasp of the quantum world.
- Often used in theoretical work, e.g., a constructive proof is used to show that something is achievable, and the converse is related to a known "no-go" theorem.

Important for building intuition of the nature of quantum information.

Re-cap: measurement in the computational basis

If we have a state $|\psi\rangle$ which is either $|0\rangle$ or $|1\rangle$, then we can perfectly distinguish which of these it is by measurement in the computational basis:

$$|1\rangle = 0\,|0\rangle + 1\,|1\rangle$$

so we measure 1 with probability $|1|^2 = 1$ (and likewise for 0).

Essentially, this is just classical (binary) information.

Distinguishing any pair of orthogonal states

If we now have a state $|\psi\rangle$ which is either $|\psi_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ or $|\psi_1\rangle = \beta^*\,|0\rangle - \alpha^*\,|1\rangle$ (where * denotes the complex conjugate), i.e., $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal, then we can still perfectly distinguish which of these it is by first performing the transformation:

$$|\phi\rangle = \begin{bmatrix} \alpha^* & \beta^* \\ \beta & -\alpha \end{bmatrix} |\psi\rangle$$

which sends $|\psi_0\rangle \to |0\rangle$ and $|\psi_1\rangle \to |1\rangle$, and then performing the measurement in the computational basis.

In fact, physicists and mathematicians frequently speak not of doing a transformation such that the states are aligned with the computational basis, but rather performing the measurement in the basis $(|\psi_0\rangle\,, |\psi_1\rangle)$, which amounts to the same thing.

It is not possible to perfectly distinguish non-orthogonal quantum states

If we now have a state $|\psi\rangle$ which is either $|\psi_a\rangle$ or $|\psi_b\rangle$ which are not orthogonal, then there is no measurement that can perfectly tell us which of these states $|\psi\rangle$ is.

... but we can perform a measurement that tells us something about the likelihood of whether $|\psi\rangle = |\psi_a\rangle$ or $|\psi\rangle = |\psi_b\rangle$.

Intuitively:

- If we just guess, we will be correct with probability equal to one half, so we expect to be able to do better than this.
- The "closer together" $|\psi_a\rangle$ and $|\psi_b\rangle$ are, the harder they will be to distinguish (i.e., the lower the probability of correctly inferring $|\psi\rangle$)

The Helstrom-Holevo Bound

The intuition in the previous slide turns out to be correct, and is captured by the Helstrom-Holevo bound:

If $|\psi\rangle$ is either $|\psi_a\rangle$ or $|\psi_b\rangle$, where $|\langle\psi_a|\psi_b\rangle| = \cos\theta$, then the probability of correctly inferring the state $|\psi\rangle$ is less than or equal to $\frac{1}{2}(1+\sin\theta)$.

Furthermore, the bound is tight, it can always be achieved by choosing the measurement basis as the eigenvectors of:

$$|\psi_a\rangle\langle\psi_a| - |\psi_b\rangle\langle\psi_b|$$

Example: distinguishing $|0\rangle$ and $|+\rangle$

First, we note that $|0\rangle$ and $|+\rangle$ are not orthogonal:

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \neq 0$$

therefore we cannot perfectly infer the state of $|\psi\rangle$ if we know it is either $|0\rangle$ or $|+\rangle$. So instead, we must decide a basis to measure in:

$$|0\rangle \langle 0| - |+\rangle \langle +| = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

which has eigenvectors $[0.38 \ 0.92]^T$ and $[-0.92 \ 0.38]^T$. Finally, we can calculate the probability of correctly inferring the state:

$$\frac{1}{2}(1 + \sin(\arccos(1/\sqrt{2}))) = 0.85$$

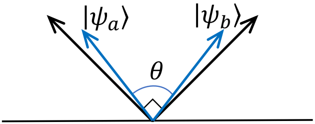
Distinguishing $|0\rangle$ and $|+\rangle$ by measuring in the computational basis

Again we have that $|\psi\rangle$ is either $|0\rangle$ or $|+\rangle$, each with 50% probability. We can tabulate the quantum states and measurement outcomes when measuring in the computational basis:

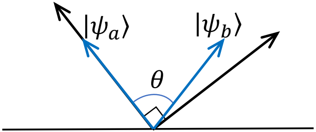
	0	1
$\|0\rangle$	$\frac{1}{2}$	0
$\|+\rangle$	$\frac{1}{4}$	$\frac{1}{4}$

- $\frac{1}{4}$ of the time we will measure 1, which means $|\psi\rangle = |+\rangle$.
- $\frac{3}{4}$ of the time we will measure 0, which we should *guess* means $|\psi\rangle = |0\rangle$, but of these $\frac{1}{3}$ will be wrong, and actually $|\psi\rangle = |+\rangle$.
- So we have success probability $1 - \frac{3}{4} \times \frac{1}{3} = \frac{3}{4}$, which is less than the theoretically achievable 0.85, but if we measure 1 then we know $|\psi\rangle = |+\rangle$ with certainty.

Depicting different state discrimination strategies



The optimal strategy is to choose the measurement basis "equally".



But if one of the measurement basis vectors aligns with one the states being distinguished, sometimes we get a measurement that we are 100% sure about.

Unambiguous state discrimination

Although detailed analysis is outside the scope of this course, it is worth being aware that there exist schemes (requiring additional ancilla qubits) which *unambiguously* discriminate non-orthogonal quantum states, but only work with some probability less than one. That is if a state $|\psi\rangle$ is either $|\psi_a\rangle$ or $|\psi_b\rangle$, the measurement outputs one of three things:

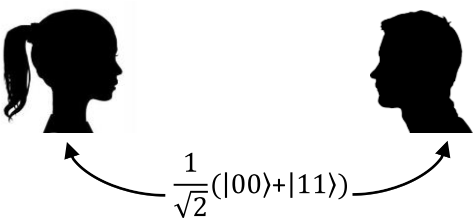
- $|\psi_a\rangle$ – in which case $|\psi\rangle$ was certainly $|\psi_a\rangle$.
- $|\psi_b\rangle$ – in which case $|\psi\rangle$ was certainly $|\psi_b\rangle$.
- 'Don't know' – in which case we have no information about $|\psi\rangle$ (which has been destroyed in the process).

The no-signalling principle: why it matters

In quantum mechanics we accept the reality of entanglement, Einstein's "spooky action at a distance", but can this be used for super-luminal information transfer, that is genuine "action at a distance", or is it merely a non-local stronger than classical correlation?

The answer is, in fact, the latter, and proven by the no-signalling principle.

The no-signalling principle: set-up



- Alice and Bob are at different ends of the universe, but each have one half of a Bell pair: $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$.
- Alice can measure her qubit whenever she wants, and this will collapse Bob's to the same state.
- We are interested in whether Bob can infer whether or not Alice has measured her qubit, if he can, then Alice can transfer information to Bob. For example, Alice can measure her qubit when some event occurs, thus *signalling* this information to Bob.
- But all that Bob can do to infer whether Alice has measured her qubit is to measure his own qubit – therefore, the question reduces to whether the measurement probabilities that Bob sees are altered by virtue of Alice having performed her measurement.

The no-signalling principle: proof

If Alice hasn't measured her qubit, then the state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and so Bob has a $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ probability of measuring each of 0 and 1.

If Alice has measured her qubit, then Bob's qubit has collapsed – it is either in state 0, or state 1 (each with probability $1/2$). However, in the absence of signalling, Bob has no knowledge of which of these measurement outcomes Alice observed, and so all he knows is that he will measure each of $|0\rangle$ and $|1\rangle$ with probability $1/2$. So the no-signalling principle is proved.

- Crucially, in the absence of signalling, Bob's measurement statistics when measuring the uncollapsed quantum state are identical to his lack of knowledge (expressed probabilistically) when measuring the state already collapsed by Alice.
- The no-signalling principle also holds for any type of entanglement, and also any scheme Alice and Bob may come up with involving transformations of their qubits, and measurements in arbitrary bases.

The no-cloning principle: why it matters

- A plethora of physics reasons.
- That we cannot clone makes quantum error-correction harder.
- The possibility of cloning would enable the violation of the no-signalling principle (see exercise sheet).
- Cloning would enable an infinite amount of classical information to be compressed into a single qubit and then recovered afterwards:
    1. Map a classical bit-string to a unique qubit state.
    2. Communicate the single qubit.
    3. Receive the qubit, make an arbitrary number of copies by cloning, and perform quantum state tomography to recover the original classical information.

The no-cloning principle: set-up

We have a quantum state $|\psi\rangle$ and a register initially set to $|0\rangle$, and we wish to find a cloning unitary, U such that:

$$U\left(|\psi\rangle\,|0\rangle\right) = |\psi\rangle\,|\psi\rangle$$

We will now prove that no such U exists.

The no-cloning principle: proof

Consider that U must clone all quantum states, so as well as

$$U\left(\left|\psi\right\rangle\left|0\right\rangle\right) = \left|\psi\right\rangle\left|\psi\right\rangle$$

from the previous slide, we have that

$$U\left(\left|\phi\right\rangle\left|0\right\rangle\right) = \left|\phi\right\rangle\left|\phi\right\rangle$$

Taking the inner products of the left- and right-hand sides of the above equations, we have that:

$$\begin{aligned}
\langle 0|\langle\psi| U^\dagger U |\phi\rangle|0\rangle =& (\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle) \\
\implies \langle\psi|\phi\rangle\langle 0|0\rangle =& (\langle\psi|\phi\rangle)^2 \\
\implies \langle\psi|\phi\rangle =& (\langle\psi|\phi\rangle)^2
\end{aligned}$$

which is only true if $\psi = \phi$ or ψ and ϕ are orthogonal (so their inner-product is 0). So we have proven that there exists no unitary U that can clone arbitrary quantum states.

The no-deleting principle

Time-reversal of the no-cloning principle yields the no-deleting principle: there does not exist a unitary $\tilde{U}$ that can delete one of two copies of a quantum state, that is:

$$\tilde{U}\left(|\psi\rangle\,|\psi\rangle\right) = |\psi\rangle\,|0\rangle$$

It is less obvious why this is useful, but the no-deleting principle does arise in quantum information, and so it is worth being aware of.

More generally, quantum computing is reversible (except for measurement), and therefore the (im)possibility of some computation implies the (im)possibility of its reverse.

Summary

In this lecture we have looked at:

- Distinguishing orthogonal and non-orthogonal states.
- Perfectly distinguishing non-orthogonal states, but with probability less than one.
- The no-signalling principle.
- The no-cloning principle.
- The no-deleting principle.