Meeting 5.2: Digging into quantum states

I. "Completely understanding" a quantum state

II. No cloning

III. Distinguishing states, redux

IV. Some good news: the Deutsch - Jozsa algorithm.

Next time: Quantum circuits as model of quantum computers, and BQP.

Note: I've given up telling myself I'm going to Tex separate notes.

Summary of axioms of quantum mechanics:

1. States are nonzero (unit) vectors in a Hilbert space.
2. Physical transformations of closed systems are unitary.
3. A quantum state $|\psi\rangle$ and measurement $\{M_0, \dots, M_k\}$ determine a probability distribution on $\{0, \dots, k\}$.
4. Composite systems are tensor products.

I. "Completely understanding" a quantum state

In classical computer with an n-bit memory register it is easy to read off information that completely determines the register's state: just read each each bit one after the other.

This is NOT true of quantum systems.

Suppose we have an n qubit system (thought of as a quantum memory) which is in a state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$.

How can we convince ourselves we completely understand $|\psi\rangle$?

It depends on $|\psi\rangle$ and what we mean by "completely understand."

One idea: determine all of the coefficients of $|\psi\rangle$ in a preferred basis.

Of course, $|\psi\rangle$ can be made part of some basis, but our "preferred basis" shouldn't depend on $|\psi\rangle$.

For n qubits, we use the tensor product basis as our computational basis.

$$|0\rangle = |00\cdots 0\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \in (\mathbb{C}^2)^{\otimes n}$$

$$|1\rangle = |00\cdots 1\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle$$

$$|2\rangle = |0\cdots 10\rangle = |0\rangle \otimes \cdots \otimes |1\rangle \otimes |0\rangle$$

$$\vdots$$

$$|N-1\rangle = |11\cdots 1\rangle = |1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle, \text{ where } N = 2^n.$$

Physical assumption: our quantum computer "knows" when its in one of these states, and can tell us which one.

In principle, we know there exist $a_0, \ldots, a_{N-1} \in \mathbb{C}$ such that

$$|\psi\rangle = \sum_{i=0}^{N-1} a_i |i\rangle, \qquad \sum_i |a_i|^2 = 1.$$

How do we determine the a_i?

Well, there are exponentially many! So let's try for a_0 only.

We need to find some measurement or observable that will help us determine a_0.

Of course,

$$a_0 = \langle 0 | \psi \rangle,$$ so we could try

$$M_0 = |0\rangle\langle 0|, \quad M_1 = I - |0\rangle\langle 0| \neq |1\rangle\langle 1|.$$

With this measurement, probability of getting outcome 0 on $|\psi\rangle$ is

$$p(0) = \langle\psi|M_0|\psi\rangle \quad \text{(note } M_0 \text{ a projector)}$$
$$= \langle\psi|0\rangle\langle 0|\psi\rangle$$
$$= a_0^* a_0$$
$$= |a_0|^2.$$

So, with this choice of measurement, the best we can do is "see" $|a_0|^2$ as a probability of a certain outcome. It turns out, with a little bit more cleverness, we could determine a_0 itself, but let's suppose we're content just to know the probability. How can we "really" do that?

Well, if we make the above measurement, either we get outcome 0 with probability $p(0) = |a_0|^2$, or we get outcome 1 with probability

$$
\begin{aligned}
p(1) &= \langle \psi | M_1 | \psi \rangle = \langle \psi | (I - |0\rangle\langle 0|) | \psi \rangle \\
&= \langle \psi | I | \psi \rangle - \langle \psi | 0 \rangle \langle 0 | \psi \rangle \\
&= |\psi|^2 - |a_0|^2 \\
&= 1 - |a_0|^2 .
\end{aligned}
$$

Performing this measurement only once, we can't expect to determine anything beyond whether it seems, probabilistically, that $|a_0|^2 \geq 1/2$ or $|a_0|^2 \leq 1/2$.

If we want to do better, we have to do another measurement!

But the First measurement spoiled $|\psi\rangle$!

If we got outcome 0, then $|\psi\rangle$ has be made into $|0\rangle$.

If we got outcome 1, then $|\psi\rangle$ is now in state

$$\frac{M_1|\psi\rangle}{\sqrt{p(1)}} = \frac{1}{\sqrt{1-|a_0|^2}}\left(|\psi\rangle - a_0|0\rangle\right) \stackrel{\cdot}{=} |1\rangle$$

In the First case, if we perform the measurement again on the new state, we of course just get back $|0\rangle$.

Likewise, in the second case,

$$M_0\left(\frac{M_1|\psi\rangle}{\sqrt{p(1)}}\right) = 0 \,, \quad M_1\left(\frac{M_1|\psi\rangle}{\sqrt{p(1)}}\right) = \frac{M_1^2|\psi\rangle}{\sqrt{p(1)}} = \frac{M_1|\psi\rangle}{\sqrt{p(1)}}.$$

So if we want to understand $|a_0|^2$ better than whether it's more likely that $|a_0|^2 \geq 1/2$ or $|a_0|^2 \leq 1/2$, we would seem to want to have another copy of $|\psi\rangle$ we could measure. We need to run our measurement experiment on $|\psi\rangle$ again.

If we had many copies of $|\psi\rangle$ at our disposal, we could do the measurement on all of them. If we did so k times then, with high probability, we can expect

$$\left| |a_0|^2 - \frac{\#\text{ of } 0 \text{ outcomes}}{k} \right| \leq O\left(\frac{1}{2^k}\right).$$

This could be made more precise...

Take-away: If we have an unlimited supply of copies of $|\psi\rangle$, we can, with high probability, approximate $|a_0|^2$ in binary reasonably efficiently.

Two issues:

1. Maybe there's a better measurement to take?

There's not.

2. What if we don't have many copies of $|\psi\rangle$?

We're sunk!

II. No cloning

Sometimes: $|0\rangle$ will mean $|0\rangle^{\otimes n}$

In short: there's no unitary way to copy quantum states.

Thm Let $n \geq m$. Then there is no ~~unitary~~ linear! transformation

$$U : \mathbb{C}^m \otimes \mathbb{C}^n \to \mathbb{C}^m \otimes \mathbb{C}^n$$

such that $U(|\psi\rangle \otimes |0\rangle^{\otimes n}) = |\psi\rangle \otimes |\psi\rangle \otimes |0\rangle^{\otimes n-m}$

for all $|\psi\rangle \in \mathbb{C}^m$.

Proof: There can't be, because

$$|\psi\rangle \otimes |0\rangle \longmapsto |\psi\rangle \otimes |\psi\rangle \otimes |0\rangle^{\otimes n-m}$$

is not linear! $\square$

So, we can only hope to "completely understand" states that we know how to prepare.

III. Distinguishing states, redux

Instead of determining $|\psi\rangle$ completely, we might be happy to have a procedure to distinguish it from all other states $|\varphi\rangle$ (so long as $|\varphi\rangle \neq e^{i\theta}|\psi\rangle$ for some $\theta \in \mathbb{R}$).

How might we go about this?

Basic idea from last time: "prepare" measurement

$$M_0 = |\psi\rangle\langle\psi| \,, \quad M_1 = I - |\psi\rangle\langle\psi| .$$

If this measurement of $|\varphi\rangle$ ever takes outcome 1, we know $|\varphi\rangle$ is not equal to $|\psi\rangle$. This procedure works, but

Many issues! Can only get around all of them in special circumstances...

1. Maybe $|\varphi\rangle = a|\psi\rangle + b|v\rangle$ $(|a|^2 + |b|^2 = 1)$ where $\langle\psi|v\rangle = 0$ and $|b|^2 = \frac{1}{2^k}$. Would expect to have to perform the measurement experiment 2^k times before we see $|\varphi\rangle$ isn't $|\psi\rangle$.

2. Just as before: need to have many copies of $|\varphi\rangle$.

3. How do we "prepare the measurement" $|\psi\rangle\langle\psi|$? Would suffice to have a way to prepare $|\psi\rangle$, i.e. a transformation that takes $|0\rangle = |0\cdots0\rangle$ to $|\psi\rangle$. Can we do better?

If $U: \mathbb{C}^n \to \mathbb{C}^n$ does $U|0\rangle = |\psi\rangle$, then

$$|\psi\rangle\langle\psi|\varphi\rangle = U|\psi\rangle\langle\psi|U^\dagger|\varphi\rangle = |0\rangle\langle 0|U^\dagger|\varphi\rangle$$

IV. Some good news: Deutsch-Jozsa algorithm

ENOUGH OF THE WARNINGS!

WHAT ARE QUANTUM STATES GOOD FOR?

Dual to the moral that a quantum state stores exponentially many classical probabilities(*), we have the philosophy:

ENTANGLEMENT IS A RESOURCE.

(*): This does NOT mean we can reliably store an exponential amount of classical information in a linear # qubits (Holevo bound)

Separable vs. Entangled states

Given a composite quantum system

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B,$$

we say a state is <u>separable</u> if it's of the form

$$|\varphi_A\rangle \otimes |\varphi_B\rangle$$

for some $|\varphi_A\rangle \in \mathcal{H}_A$, $|\varphi_B\rangle \in \mathcal{H}_B$.

If $|\varphi\rangle \in \mathcal{H}_{AB}$ is not separable, it is <u>entangled</u>.

Deutsch's Problem

Input: a black box function

$$F: \{0,1\}^n \longrightarrow \{0,1\}$$

which is promised to be either:

i) constant, or

ii) balanced, meaning $\# F^{-1}(0) = \# F^{-1}(1)$.

Problem: Decide whether F is constant or balanced.

Classically, requires $2^{n-1}+1$ evaluations of F.

If we have access to "quantum black box function" for f, we can solve the problem in ~~constant~~ time!

linear?

$$U_f : (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n}$$

$$|x\rangle \otimes \underbrace{|y\rangle}_{\text{ancilla qubits}} \longmapsto |x\rangle \otimes |y \oplus f(x)\rangle$$

$\oplus$: Boolean addition of bit strings

This flips y's first (zu) bit if $f(x)=1$ or does nothing in $f(x)=0$.

$$U_f^{-1} = U_f.$$

Details: (Nielsen - Chuang)

Algorithm: Deutsch–Jozsa

Inputs: (1) A black box U_f which performs the transformation $|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$, for $x \in \{0, \dots, 2^n - 1\}$ and $f(x) \in \{0, 1\}$. It is promised that $f(x)$ is either *constant* for all values of x, or else $f(x)$ is *balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs: 0 if and only if f is constant.

Runtime: One evaluation of U_f. Always succeeds.

Procedure:

entangled state

1. $|0\rangle^{\otimes n}|1\rangle$ — initialize state
2. $\to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ — create superposition using Hadamard gates
3. $\to \sum_x (-1)^{f(x)} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ — calculate function f using U_f
4. $\to \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}|z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ — perform Hadamard transform
5. $\to z$ — measure to obtain final output z

Caveats:

1. Contrived problem
2. Deutsch's problem can be efficiently solved with high probability on a classical probabilistic computer (meaning the algorithm can flip coins)
3. Apples and oranges: "black box" vs. "quantum black box"