CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Tuesday, January 23 - Lecture 3.1

Today's scribe: Eduardo

Reading: Subsection 2.2 of Nielsen and Chuang.

Agenda:

1. Projective measurements
2. Quantum state tomography
3. Distinguishing states
4. Uncertainty principle
5. Global phases and complex projective space

1 Projective measurements (Born rule)

Last time we saw that a projective measurement is a self-adjoint operator, i.e.,

$$M^* = M.$$

Thus, we can write its spectral decomposition

$$M = \sum_i \lambda_i P_i,$$

where λ_i are the distinct eigenvalues and P_i are the orthogonal projections onto the λ_i subspace.

The outcomes of this measurement are the λ_i eigenvalues. The probability of seeing these eigenvalues given that we are on a state $|\psi\rangle$ are

$$\Pr(\lambda_i || \psi\rangle) = \frac{\langle \psi | P_i | \psi \rangle}{\langle \psi | \psi \rangle} \tag{1}$$

which is basically the normalized size of $|\psi\rangle$ on the λ_i eigenspace.

Examples. Measuring in the computational basis of n qubits

1. Let $\mathscr{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ and $M = \sum_{b=0}^{2^n-1} b|b\rangle\langle b|$.
   Observe that if $n = 1$
   $$M = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$
   and if $n = 2$
   $$M = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}.$$

Note that M is already diagonal in the computational basis. The outcomes if we measure M are its eigenvalues, i.e.,

$$\{0, 1, 2, \ldots, 2^n - 1\}.$$

What is $\Pr(i || \psi\rangle)$ if $|\psi\rangle = \sum_i z_i |i\rangle \neq \vec{0}$? By applying Equation (1) we get

$$\Pr(i||\psi\rangle) = \frac{z_i z_i^*}{\sum_j z_j z_j^*}. \tag{2}$$

2. Suppose $n = 1$ and

$$|\psi\rangle = \frac{3|0\rangle - i|1\rangle}{\sqrt{7}}.$$

Then, by applying Equation (2) we get

$$\begin{aligned}\Pr(0||\psi\rangle) &= \frac{\frac{3\cdot 3^*}{7}}{\left(\frac{3}{\sqrt{7}}\right)\left(\frac{3}{\sqrt{7}}\right) + \left(\frac{-i}{\sqrt{7}}\right)\left(\frac{i}{\sqrt{7}}\right)} \\ &= \frac{\frac{9}{7}}{\frac{9}{7} + \frac{1}{7}} \\ &= \frac{9}{10}.\end{aligned}$$

Note that we get for free

$$\begin{aligned}\Pr(1||\psi\rangle) &= 1 - \Pr(0||\psi\rangle) \\ &= \frac{1}{10}\end{aligned}$$

by the complement rule.

Remark. *We should stress that the measurement together with the state induces a probability distribution on the set of all bit strings that is entirely determined by the amplitudes of z_i by Equation (2).*

3. Recall from last class that

$$H^{\otimes n}|0\ldots 0\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{b=0}^{2^n - 1} |b\rangle,$$

where H is the Hadamard operator.

In particular,

$$\Pr(i||\psi\rangle) = \frac{1}{2^n},$$

where $|\psi\rangle = |0\ldots 0\rangle$.

Now let $\theta_0, \ldots, \theta_{2^n - 1} \in \mathbb{R}$, and define

$$|\psi(\theta_0, \ldots, \theta_{2^n-1})\rangle = \frac{1}{2^{n/2}} \sum_{b=0}^{2^n-1} e^{2\pi j \theta_b} |b\rangle.$$

Note that

$$|\psi(\theta_0, \ldots, \theta_{2^n-1})\rangle \neq |\psi\rangle,$$

but it turns out that

$$\Pr(i||\psi(\vec{\theta})\rangle) = \Pr(i||\psi\rangle).$$

Thus, if we measure in the computational basis we get the same probability distribution, even though the states are different. This means that there is more to a quantum state than just the probability distribution on bit strings we get by measuring in the computational basis.

2 Quantum state tomography

Quantum state tomography is the procedure of experimentally determining an unknown quantum state. The challenge lies in the inherently probabilistic nature of observations in quantum systems, where a single copy of a state $|\psi\rangle$ can only give us one sample of its distribution. How many copies of $|\psi\rangle$ do we need to learn something non-trivial about its amplitudes (in computational basis) with high confidence?

This is not so different from the problem of estimating the probability of outcomes in an unfair coin. In particular, how many times do we need to flip the coin to get an approximation of the probability of getting heads or tails? We can never be certain that we have the best approximation for such probabilities, but we can approach an accurate estimation within a certain confidence interval.

One might also ask: Is possessing a biased coin equivalent to knowing its bias? Or, does the coin "know" its own bias? We can argue that knowing the bias is not inherent in the coin; it requires experimentation to extract this information, and even then, it's determined only within a certain confidence interval.

In other words, having a quantum state $|\psi\rangle = \sum z_i |i\rangle$ and not knowing the amplitudes z_i is similar to having a biased coin and not knowing what the bias is.

3 Distinguishing quantum states

Suppose $|\psi\rangle, |\phi\rangle \in \mathscr{H}$, where $\mathscr{H} \cong \mathbb{C}^d$.

Question: Is there a (projective) measurement we can perform to distinguish $|\psi\rangle$ from $|\phi\rangle$ with certainty in "one shot" ?

Answer: Yes, if and only if $\langle\phi|\psi\rangle = 0$, i.e., the states are orthogonal. We will prove this statement.

($\Leftarrow$) Let

$$M = \underbrace{|\psi\rangle\langle\psi|}_{P_1} + 2\underbrace{|\phi\rangle\langle\phi|}_{P_2}.$$

Observe that M is already written in its spectral form. If we perform a projective measurement of M on a state $|x\rangle$ that is equal to either $|\phi\rangle$ or $|\psi\rangle$ (we will assume that both states are already normalized), then

$$\begin{aligned}\Pr(1||x\rangle) &= \langle x|P_1|x\rangle \\ &= \begin{cases} 1, & \text{if } |x\rangle = |\psi\rangle, \\ 0, & \text{if } |x\rangle = |\phi\rangle, \end{cases}\end{aligned}$$

and

$$\begin{aligned}\Pr(2||x\rangle) &= \langle x|P_2|x\rangle \\ &= \begin{cases} 0, & \text{if } |x\rangle = |\psi\rangle, \\ 1, & \text{if } |x\rangle = |\phi\rangle. \end{cases}\end{aligned}$$

Thus, performing this measurement will tell us with certainty what $|x\rangle$ is[1].

We should note that this is a "bad" answer in the sense that we need to know what states are. Thus, this answer is more informational-theoretic than algorithmic.

($\Rightarrow$) By contradiction suppose that $\langle\phi|\psi\rangle \neq 0$ and M is an observable with two distinguished outcomes "1" and "2" such that

$$\Pr(1||\psi\rangle) = 1,$$

$$\Pr(2||\psi\rangle) = 0,$$

[1]Note that $\lambda = 0$ is also an eigenvalue of M, but since $|x\rangle \in \{|\psi\rangle, |\phi\rangle\}$ we will never observe this outcome

$$\Pr(1||\phi\rangle) = 0,$$

and

$$\Pr(2||\phi\rangle) = 1.$$

Then,

$$M|_{\mathrm{span}\{|\phi\rangle,|\psi\rangle\}} = 1 \cdot P_1 + 2 \cdot P_2$$

for some projectors P_1 and P_2. Note

$$\begin{aligned} P_1 + P_2 &= I \\ &= I_{\mathrm{span}\{|\phi\rangle,|\psi\rangle\}}. \end{aligned}$$

Applying the Born rule,

$$\begin{aligned} \Pr(1||\psi\rangle) &= \langle\psi|P_1|\psi\rangle, \\ \Pr(2||\psi\rangle) &= \langle\psi|P_2|\psi\rangle, \\ \Pr(1||\phi\rangle) &= \langle\phi|P_1|\phi\rangle \end{aligned}$$

and

$$\Pr(2||\phi\rangle) = \langle\phi|P_2|\phi\rangle.$$

Write

$$|\phi\rangle = \alpha|\psi\rangle + \beta|\psi^\perp\rangle,$$

where $\langle\psi|\psi^\perp\rangle = 0$, and $|\alpha|^2 + |\beta|^2 = 1$, $\beta \neq 0$ and $\alpha \neq 0$. Then,

$$\begin{aligned} 1 &= \langle\phi|P_2|\phi\rangle \\ &= (\alpha^*\langle\psi| + \beta^*\langle\psi^\perp|)P_2(\alpha|\psi\rangle + \beta|\psi^\perp\rangle) \\ &= \alpha^*\alpha\underbrace{\langle\psi|P_2|\psi\rangle}_{0} + \beta^*\beta\underbrace{\langle\psi^\perp|P_2|\psi^\perp\rangle}_{1} \end{aligned}$$

Thus, $|\beta^*\beta| = 1$, which implies $\alpha = 0$. This contradicts our assumption $\langle\psi|\phi\rangle \neq 0$.

Note the contrast with the $\Leftarrow$ direction, where knowing what the states were allowed us to build a measurement M from which we can distinguish the states with certainty. Here, even knowing the states, there is no way to distinguish the states with certainty due to the non-orthogonality between $|\psi\rangle$ and $|\phi\rangle$.

4 Uncertainty principle

Projective measurements have a very clean formula for expectation values (i.e., averages).

$$\begin{aligned} \mathbb{E}(M||\psi\rangle) &= \sum_{\lambda \text{ is eigenvalue of } M} \lambda \Pr(\lambda||\psi\rangle) \\ &= \sum_\lambda \lambda\langle\psi|P_\lambda|\psi\rangle \\ &= \langle\psi|\left(\sum_\lambda \lambda P_\lambda\right)|\psi\rangle \\ &= \langle\psi|M|\psi\rangle \end{aligned}$$

In particular, we don't need to know spectral decomposition of M to compute

$$\mathbb{E}(M||\psi\rangle) = \langle\psi|M|\psi\rangle.$$

Sometimes, when $|\psi\rangle$ is understood, we write

$$\langle M\rangle := \mathbb{E}(M|\psi\rangle).$$

From this,

$$\begin{aligned}\mathrm{Var}(M)_{|\psi\rangle} &= \mathrm{Var}(M)\\ &= \mathbb{E}\left[M-(\mathbb{E}(M))^2\right]\\ &= \mathbb{E}(M^2)-(\mathbb{E}(M))^2\\ &= \langle M^2\rangle - \langle M\rangle^2\end{aligned}$$

Thus, the standard deviation is

$$\Delta(M) = \Delta(M)_{|\psi\rangle} = \sqrt{\mathrm{Var}(M)}.$$

Note. $\Delta(M)_{|\psi\rangle} = 0$ *if and only if* $|\psi\rangle$ *is an eigenvector of* M.

Heisenberg uncertainty principle:

For all observables A and B,

$$\Delta(A)_{|\psi\rangle}\Delta(B)_{|\psi\rangle} \geq \frac{1}{2}\langle\psi|[A,B]|\psi\rangle.$$

Intuitively, this is saying that if we want the product of the two standard deviations of two operators to be small, then they should be very close to commuting on state $|\psi\rangle$.

Remark. *This statement is not saying that performing one measurement affects the outcome of another.*

In particular, one can only be ever certain about the outcomes of both A and B on $|\psi\rangle$ if they "commute on $|\psi\rangle$". Note that if we are certain about the outcomes of A and B, then $\Delta(A)|_{|\psi\rangle} = \Delta(B)_{|\psi\rangle} = 0$. This means that $|\psi\rangle$ is an eigenvector of both A and B, and thus $[A,B]|\psi\rangle = 0$.

5 Global phases and complex projective space

Global phases don't matter. That is, if $|\phi\rangle = z|\psi\rangle$ for some $z \in \mathbb{C}-\{0\}$, then there is no measurement that can distinguish $|\phi\rangle$ from $|\psi\rangle$, and so, we should consider $|\phi\rangle$ and $|\psi\rangle$ as the same state [2].

Let $M = \sum \lambda P_\lambda$ be any projective measurement. Then,

$$\begin{aligned}\Pr(\lambda||\phi\rangle) &= \frac{\langle\phi|P_\lambda|\phi\rangle}{\langle\phi|\phi\rangle}\\ &= \frac{(z^*\langle\psi|)P_\lambda(z|\psi\rangle)}{(z^*\langle\psi|)(z|\psi\rangle)}\\ &= \frac{\langle\psi P_\lambda|\psi\rangle}{\langle\psi|\psi\rangle}\\ &= \Pr(\lambda||\psi\rangle).\end{aligned}$$

Thus, if these two distributions are always the same whenever we perform a measurement no matter what the measurement is, it makes sense to regard them as being the same state.

[2] In particular, this is why we don't care about normalization because normalization is just multiplying by a non-zero scalar.

If we consider a qudit $\mathbb{C}^d$, we have said that $\mathbb{C}^d - \{0\}$ is the space where quantum states are allowed to be. Now we are also saying that two different states that differ by some scalar factor are the same. This means that what really parametrizes quantum states (and that does so in a one-to-one manner) is the quotient $\mathbb{C}^d - \{0\}/\mathbb{C} - \{0\}$, which is exactly the projective space $\mathbb{CP}^{d-1}$, i.e.,

$$\mathbb{C}^d - \{0\}/\mathbb{C} - \{0\} \cong \mathbb{CP}^{d-1}.$$

Note that $\mathbb{CP}^{d-1}$ is essentially the set of lines of complex lines in $\mathbb{C}^d$.

Thus, the set of pure states is in fact bijective with the complex projective space. In particular, when $d = 2$, $\mathbb{CP}^1$ is homeomorphic and isometric with the two dimensional sphere that is called that Bloch sphere.