CS 593/MA 595 - Introduction to Quantum Computing

Quantum Computation and Quantum Information by *Isaac Chuang, Michael Nielsen*
Student: **Ralph Razzouk**

Homework 2

Problem 2.57
(Cascaded measurements are single measurements) Suppose $\{L_l\}$ and $\{M_m\}$ are two sets of measurement operators. Show that a measurement defined by the measurement operators $\{L_l\}$ followed by a measurement defined by the measurement operators $\{M_m\}$ is physically equivalent to a single measurement defined by measurement operators $\{N_{lm}\}$ with the representation $N_{lm} \equiv M_m L_l$.

Proof. Consider a normalized initial quantum state $|\psi_0\rangle$. The state $|\psi_0\rangle$, after of measurement of L_l is given, by definition, to be

$$|\psi_0\rangle \mapsto |\psi_1\rangle = \frac{L_l |\psi_0\rangle}{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger L_l \middle| \psi_0 \right\rangle}}.$$

The state $|\psi_1\rangle$, after of measurement of M_m, is given to be

$$\begin{aligned}
|\psi_1\rangle \mapsto |\psi_2\rangle &= \frac{M_m |\psi_1\rangle}{\sqrt{\left\langle \psi_1 \middle| M_m^\dagger M_m \middle| \psi_1 \right\rangle}} \\
&= \frac{M_m \left(\frac{L_l |\psi_0\rangle}{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger L_l \middle| \psi_0 \right\rangle}} \right)}{\sqrt{\left\langle \frac{L_l^\dagger \langle \psi_0|}{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger L_l \middle| \psi_0 \right\rangle}} \middle| M_m^\dagger M_m \middle| \frac{L_l |\psi_0\rangle}{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger L_l \middle| \psi_0 \right\rangle}} \right\rangle}} \\
&= \frac{M_m L_l |\psi_0\rangle}{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger L_l \middle| \psi_0 \right\rangle}} \frac{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger L_l \middle| \psi_0 \right\rangle}}{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger M_m^\dagger M_m L_l \middle| \psi_0 \right\rangle}} \\
&= \frac{M_m L_l |\psi_0\rangle}{\sqrt{\left\langle \psi_0 \middle| L_l^\dagger M_m^\dagger M_m L_l \middle| \psi_0 \right\rangle}}.
\end{aligned}$$

If we define $N_{lm} \equiv M_m L_l$, then the state $|\psi_0\rangle$, after measurement of N_{lm}, is equivalent to the state $|\psi_2\rangle$. In other words, the state $|\psi_2\rangle$, after the measurement of N_{lm}, yields the same state. ∎

Problem 2.58
Suppose we prepare a quantum system in an eigenstate $|\psi\rangle$ of some observable M, with corresponding eigenvalue m. What is the average observed value of M, and the standard deviation?

Proof. By the definition of the expectation value, we have

$$\begin{aligned}
\langle M \rangle_{|\psi\rangle} &= \langle \psi | M | \psi \rangle \\
&= \langle \psi | m | \psi \rangle \quad \text{(definition of eigenvalue)} \\
&= m \langle \psi | \psi \rangle \\
&= m \qquad \text{(normalized quantum state).}
\end{aligned}$$

Calculating the expectation value of the square, we have

$$\begin{aligned}\left\langle M^2\right\rangle_{|\psi\rangle} &= \left\langle\psi\middle|M^2\middle|\psi\right\rangle \\ &= \langle\psi|MM|\psi\rangle \\ &= m\,\langle\psi|M|\psi\rangle \\ &= m^2\,\langle\psi|\psi\rangle \\ &= m^2.\end{aligned}$$

Calculating the standard deviation, we have

$$\Delta(M) = \sqrt{\langle M^2\rangle - \langle M\rangle^2} = \sqrt{m^2 - m^2} = 0.$$

■

Problem 2.59
Suppose we have qubit in the state $|0\rangle$, and we measure the observable X. What is the average value of X? What is the standard deviation of X?

Proof. The expectation value of X is

$$\begin{aligned}\langle X\rangle_{|0\rangle} &= \langle 0|X|0\rangle \\ &= \langle 0|1\rangle \quad \text{(definition of } X\text{)} \\ &= 0.\end{aligned}$$

Calculating the expectation value of the square, we have

$$\begin{aligned}\left\langle X^2\right\rangle_{|0\rangle} &= \left\langle 0\middle|X^2\middle|0\right\rangle \\ &= \langle 0|XX|0\rangle \\ &= \langle 0|X|1\rangle \\ &= \langle 0|0\rangle \\ &= 1.\end{aligned}$$

Calculating the standard deviation, we have

$$\Delta(X) = \sqrt{\langle X^2\rangle - \langle X\rangle^2} = \sqrt{1-0} = 1.$$

■

Problem 2.60
Show that $\vec{v}\cdot\vec{\sigma}$ has eigenvalues ± 1, and that the projectors onto the corresponding eigenspaces are given by $P_\pm = (I \pm \vec{v}\cdot\vec{\sigma})/2$.

Proof. Let $|v\rangle$ be a unit vector and $|\sigma\rangle = (\sigma_1, \sigma_2, \sigma_3)$, where σ_i are the Pauli's sigma matrices. First, we compute $\vec{v}\cdot\vec{\sigma}$

$$\vec{v}\cdot\vec{\sigma} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 = v_1\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} + v_2\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} + v_3\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}v_3 & v_1 - iv_2\\ v_1 + iv_2 & -v_3\end{bmatrix}.$$

Using the characteristic equation to find the eigenvalues, we have

$$\begin{aligned}
\det(\vec{v}\cdot\vec{\sigma} - \lambda\mathbb{I}) &= 0 \\
\begin{vmatrix} v_3 - \lambda & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 - \lambda \end{vmatrix} &= 0 \\
-(v_3 + \lambda)(v_3 - \lambda) - (v_1 + iv_2)(v_1 - iv_2) &= 0 \\
\lambda^2 - (v_1^2 + v_2^2 + v_3^2) &= 0 \\
\lambda^2 - 1 &= 0 \quad (\text{since } |v\rangle \text{ is a unit vector}) \\
\lambda_\pm &= \pm 1.
\end{aligned}$$

Finding the eigenvectors, we have

- For $\lambda_- = -1$:

$$(\vec{v}\cdot\vec{\sigma} - \lambda_-\mathbb{I})\,|\lambda_-\rangle = 0 \begin{pmatrix} v_3 + 1 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 + 1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 0$$

$$\implies \begin{cases} (v_3+1)\alpha + (v_1 - iv_2)\beta = 0 \\ (v_1 + iv_2)\alpha + (-v_3+1)\beta = 0 \end{cases}$$

$$\implies \begin{cases} \beta = \frac{v_1 + iv_2}{v_3 - 1}\alpha \\ \alpha = v_3 - 1 \text{ (arbitrary)} \end{cases}$$

$$\begin{aligned}
|\lambda_-\rangle &= \frac{1}{\sqrt{|v_3 - 1|^2 + |v_1 + iv_2|^2}}\begin{pmatrix} v_3 - 1 \\ v_1 + iv_2 \end{pmatrix} \\
&= \frac{1}{\sqrt{v_3^2 - 2v_3 + 1 + v_1^2 + v_2^2}}\begin{pmatrix} v_3 - 1 \\ v_1 + iv_2 \end{pmatrix} \\
&= \frac{1}{\sqrt{2(1 - v_3)}}\begin{pmatrix} v_3 - 1 \\ v_1 + iv_2 \end{pmatrix}
\end{aligned}$$

Let P_- be the projector of $|\lambda_-\rangle$, then

$$\begin{aligned}
P_- &= |\lambda_-\rangle\langle\lambda_-| \\
&= \frac{1}{2(1 - v_3)}\begin{pmatrix} v_3 - 1 \\ v_1 + iv_2 \end{pmatrix}\begin{pmatrix} v_3 - 1 & v_1 - iv_2 \end{pmatrix} \\
&= \frac{1}{2(1 - v_3)}\begin{pmatrix} (v_3 - 1)^2 & (v_3 - 1)(v_1 - iv_2) \\ (v_1 + iv_2)(v_3 - 1) & (v_1 + iv_2)(v_1 - iv_2) \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 - v_3 & -v_1 + iv_2 \\ -v_1 - iv_2 & \frac{v_1^2 + v_2^2}{1 - v_3} \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 - v_3 & -v_1 + iv_2 \\ -v_1 - iv_2 & \frac{1 - v_3^2}{1 - v_3} \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 - v_3 & -v_1 + iv_2 \\ -v_1 - iv_2 & 1 + v_3 \end{pmatrix} \\
&= \frac{1}{2}(\mathbb{I} - \vec{v}\cdot\vec{\sigma})
\end{aligned}$$

- For $\lambda_+ = 1$:

$$(\vec{v}\cdot\vec{\sigma} - \lambda_+\mathbb{I})\,|\lambda_+\rangle = 0 \begin{pmatrix} v_3 - 1 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 - 1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 0$$

$$\implies \begin{cases} (v_3-1)\alpha + (v_1 - iv_2)\beta = 0 \\ (v_1+iv_2)\alpha + (-v_3-1)\beta = 0 \end{cases}$$

$$\implies \begin{cases} \beta = \frac{v_1+iv_2}{v_3+1}\alpha \\ \alpha = v_3 + 1 \text{ (arbitrary)} \end{cases}$$

$$\begin{aligned} |\lambda_+\rangle &= \frac{1}{\sqrt{|v_3+1|^2 + |v_1+iv_2|^2}}\begin{pmatrix} v_3+1 \\ v_1+iv_2 \end{pmatrix} \\ &= \frac{1}{\sqrt{v_3^2+2v_3+1+v_1^2+v_2^2}}\begin{pmatrix} v_3+1 \\ v_1+iv_2 \end{pmatrix} \\ &= \frac{1}{\sqrt{2(1+v_3)}}\begin{pmatrix} v_3+1 \\ v_1+iv_2 \end{pmatrix} \end{aligned}$$

Let P_+ be the projector of $|\lambda_+\rangle$, then

$$\begin{aligned} P_+ &= |\lambda_+\rangle\langle\lambda_+| \\ &= \frac{1}{2(1+v_3)}\begin{pmatrix} v_3+1 \\ v_1+iv_2 \end{pmatrix}\begin{pmatrix} v_3+1 & v_1-iv_2 \end{pmatrix} \\ &= \frac{1}{2(1+v_3)}\begin{pmatrix} (v_3+1)^2 & (v_3+1)(v_1-iv_2) \\ (v_1+iv_2)(v_3+1) & (v_1+iv_2)(v_1-iv_2) \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1+v_3 & v_1-iv_2 \\ v_1+iv_2 & \frac{v_1^2+v_2^2}{1+v_3} \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1+v_3 & v_1-iv_2 \\ v_1+iv_2 & \frac{1-v_3^2}{1+v_3} \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1+v_3 & v_1-iv_2 \\ v_1+iv_2 & 1-v_3 \end{pmatrix} \\ &= \frac{1}{2}(\mathbb{I} + \vec{v}\cdot\vec{\sigma}) \end{aligned}$$

Thus,

$$P_\pm = \frac{1}{2}(\mathbb{I} \pm \vec{v}\cdot\vec{\sigma})$$

as claimed. ■

Problem 2.61
Calculate the probability of obtaining the result $+1$ for a measurement of $\vec{v}\cdot\vec{\sigma}$, given that the state prior to measurement is $|0\rangle$. What is the state of the system after the measurement if $+1$ is obtained?

Proof. From Problem 2.60, we have

$$P_\pm = \frac{1}{2}(\mathbb{I} \pm \vec{v}\cdot\vec{\sigma})$$

where

$$\vec{v}\cdot\vec{\sigma} = \begin{bmatrix} v_3 & v_1-iv_2 \\ v_1+iv_2 & -v_3 \end{bmatrix} = v_3\,|0\rangle\langle 0| + (v_1-iv_2)\,|0\rangle\langle 1| + (v_1+iv_3)\,|1\rangle\langle 0| - v_3\,|1\rangle\langle 1|$$

The probability of obtaining the result +1 given that the state prior to measurement is $|0\rangle$ is

$$\begin{aligned}
p(+1) &= \langle 0|P_+|0\rangle \\
&= \frac{1}{2}\langle 0|\mathbb{I}+\vec{v}\cdot\vec{\sigma}|0\rangle \\
&= \frac{1}{2}\left[\langle 0|\mathbb{I}|0\rangle + \langle 0|\vec{v}\cdot\vec{\sigma}|0\rangle\right] \\
&= \frac{1}{2}\left[1 + \langle 0|v_3|0\rangle + \langle 0|(v_1+iv_3)|1\rangle\right] \\
&= \frac{1+v_3}{2}.
\end{aligned}$$

The state of the system after the measurement if +1 is obtained is

$$|0\rangle \mapsto \frac{P_+|0\rangle}{\sqrt{p(+1)}} = \frac{\frac{1+v_3}{2}|0\rangle + \frac{v_1+iv_2}{2}|1\rangle}{\sqrt{\frac{1+v_3}{2}}} = \frac{(1+v_3)|0\rangle + (v_1+iv_2)|1\rangle}{\sqrt{2(1+v_3)}}.$$

■

Problem 2.66
Show that the average value of the observable X_1Z_2 for a two qubit system measured in the state $(|00\rangle + |11\rangle)/\sqrt{2}$ is zero.

Proof. The expectation value of the observable X_1Z_2 when measured in the state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is

$$\begin{aligned}
\langle X_1Z_2\rangle &= \left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) X_1Z_2 \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{2}\left(\langle 00| + \langle 11|\right)\left(X_1Z_2|00\rangle + X_1Z_2|11\rangle\right) \\
&= \frac{1}{2}\left(\langle 00| + \langle 11|\right)\left(X_1|00\rangle - X_1|11\rangle\right) \\
&= \frac{1}{2}\left(\langle 00| + \langle 11|\right)\left(|10\rangle - |01\rangle\right) \\
&= \frac{1}{2}\left(\langle 00|10\rangle - \langle 00|01\rangle + \langle 11|10\rangle - \langle 11|01\rangle\right) \\
&= 0.
\end{aligned}$$

■

Problem 2

(a) A vector $|\psi\rangle$ in a tensor product Hilbert space $V\otimes W$ is called *separable* (or *unentangled*) if there exist vectors $|v\rangle \in V$ and $|w\rangle \in W$ such that $|\psi\rangle = |v\rangle \otimes |w\rangle$. Give an example of a state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes 2}$ on two qubits that is not separable (in other words, it is entangled). Justify your answer.

(b) Show that $V\otimes W$ has no entangled states if and only if V or W is 0 or 1 dimensional.

Proof. (a) The most common example of an entangled state is the Bell state $|\psi\rangle = \frac{1}{2}(|00\rangle + |11\rangle)$.

To determine if the pure state is entangled, one could try a brute force method of attempting to find satisfying states $|v\rangle \in V$ and $|w\rangle \in W$ such that $|\psi\rangle = |v\rangle \otimes |w\rangle$. This is inelegant, and hard work in the general case. A more straightforward way to prove whether this pure state is entangled is the calculate the reduced density matrix ρ for one of the qubits, i.e. by tracing out the other. The state is separable if and only if ρ has rank 1. Otherwise it is entangled. Mathematically, we can test the rank condition simply by evaluating $\mathrm{Tr}(\rho^2)$. The original state is separable if and only if this value is 1. Otherwise the state is entangled.

Suppose we have a pure separable state $|\phi\rangle = |v\rangle \otimes |w\rangle$. The reduced density matrix is

$$\rho = \mathrm{Tr}(|\phi\rangle\langle\phi|) = |v\rangle\langle v|,$$

and

$$\mathrm{Tr}(\rho^2) = \mathrm{Tr}(|v\rangle\langle v| \cdot |v\rangle\langle v|) = \mathrm{Tr}(|v\rangle\langle v|) = 1.$$

Thus, we have a separable state.

Considering our Bell state $|\psi\rangle$, then

$$\rho = \mathrm{Tr}(|\psi\rangle\langle\psi|) = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) = \frac{1}{2}\mathbb{I},$$

and

$$\mathrm{Tr}(\rho^2) = \frac{1}{4}\mathrm{Tr}(\mathbb{I}\cdot\mathbb{I}) = \frac{1}{2} \neq 1$$

Thus, the Bell state is not a separable state and is, hence, entangled.

(b) Suppose that $\dim(V) = m$ and $\dim(W) = n$.

$\boxed{\implies}$ Suppose the product $V \otimes W$ has no entangled states. Then, for every element $|\psi\rangle \in V \otimes W$, there exists vectors $|v\rangle \in V$ and $|w\rangle \in W$ such that $|\psi\rangle = |v\rangle \otimes |w\rangle$.

Let us assume that $\dim(V) = m \geq 2$ and $\dim(W) = n \geq 2$ and suppose that $\{|v_1\rangle, |v_2\rangle\}$ are linearly independent in V and that $\{|w_1\rangle, |w_2\rangle\}$ are linearly independent in W. Seeking a contradiction, suppose that

$$|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle = |v\rangle \otimes |w\rangle. \tag{1}$$

Extending $\{|v_1\rangle, |v_2\rangle\}$ to a basis $\{|v_1\rangle, |v_2\rangle, \dots, |v_m\rangle\}$ of V and $\{|w_1\rangle, |w_2\rangle\}$ to a basis $\{|w_1\rangle, |w_2\rangle, \dots, |w_n\rangle\}$ of W, we have

$$|v\rangle = \alpha_1|v_1\rangle + \alpha_2|v_2\rangle + \cdots + \alpha_m|v_m\rangle$$
$$|w\rangle = \beta_1|w_1\rangle + \beta_2|w_2\rangle + \cdots + \beta_n|w_n\rangle$$

$$\implies |v\rangle \otimes |w\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_i\beta_j |v_i\rangle \otimes |w_j\rangle. \tag{2}$$

Since the tensor product $V \otimes W$ has no entangled states, then a valid basis for the tensor product space is

$$\mathcal{B} = \{|v_i\rangle \otimes |v_j\rangle \,|1 \leq i \leq m, 1 \leq j \leq n\}.$$

From the equations (1) and (2), we have that

$$\alpha_i\beta_j = \begin{cases} 1, & \text{for } i,j = 1 \\ 1, & \text{for } i,j = 2 \\ 0, & \text{otherwise} \end{cases} \implies \alpha_i = \begin{cases} 1, & \text{for } i = 1,2 \\ 0, & \text{for } i \neq 1,2 \end{cases}, \quad \beta_j = \begin{cases} 1, & \text{for } j = 1,2 \\ 0, & \text{for } j \neq 1,2 \end{cases}.$$

We may now write equation (1) as

$$\begin{aligned} |v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle &= |v\rangle \otimes |w\rangle \\ &= (|v_1\rangle + |v_2\rangle) \otimes (|w_1\rangle + |w_2\rangle) \\ &= |v_1\rangle \otimes |w_1\rangle + |v_1\rangle \otimes |w_2\rangle + |v_2\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle \end{aligned}$$

which contradicts that $\mathcal{B}$ is a basis for $V \otimes W$.

Therefore, if the tensor product space $V \otimes W$ has no entangled states, then $\dim(V) = m \leq 1$ or $\dim(W) = n \leq 1$.

$\boxed{\Longleftarrow}$

- Without loss of generality, suppose that V is zero-dimensional. Then it must be that $|v\rangle = \mathbf{0}$ is the only element in V. Then any $|\psi\rangle \in V \otimes W$ is of the form

  $$|\psi\rangle = \mathbf{0} \otimes |w\rangle = \mathbf{0}.$$

  In addition, $\mathbf{0}$ is always separable. In fact

  $$\mathbf{0} \otimes \mathbf{0} = \mathbf{0}.$$

  Thus, the tensor product space $V \otimes W$, where V or W is zero-dimensional, has no entangled states.
- Without loss of generality, suppose that V is one-dimensional. Then it must be that $|v\rangle = \alpha\,|0\rangle$. Then any $|\psi\rangle \in V \otimes W$ is of the form

  $$|\psi\rangle = |v\rangle \otimes |w\rangle = \alpha\,|0\rangle \otimes \sum_{j=1}^{n} \beta_j\,|w_j\rangle\,,$$

  which is always separable.
  Thus, the tensor product space $V \otimes W$, where V or W is one-dimensional, has no entangled states.

Therefore, if V or W is zero or one dimensional, then the tensor product space $V \otimes W$ has no entangled states.

■

Problem 3
Let's work through the details of quantum state tomography via repeated measurements in the computational basis.

Let
$$|\psi\rangle = \sum_{b=0}^{2^n-1} z_b\,|b\rangle \in (\mathbb{C}^2)^{\otimes 2}$$
be some unknown state on n qubits, which we will assume is normalized. The goal of quantum state tomography is to determine what the amplitudes z_b are—up to a given error, with high confidence. We don't yet have the tools to do things at this level of precision quite yet, but we can at least ask about trying to determine, say, $|z_0|^2$ up to some given accuracy.

Since measurement collapses the state, we will assume that we are able to prepare copies of this state for free. On each copy, we will perform projective measurement in the computational basis. The outcomes will be independent and identically distributed. If we do this k times, we get a sequence of outcomes $(i_1, \ldots, i_k)$ where each $i_j \in \{0, \ldots, 2^n - 1\}$. From this, we may compute an empirical probability distribution $\tilde{p}_k$ on the set $\{0, \ldots, 2^n - 1\}$ simply by counting the different outcomes and dividing by k
$$\tilde{p}_k(i) := \frac{\#\{j|i_j = i\}}{k}. \tag{3}$$

Of course, the *true* distribution of outcomes is given by the Born rule:
$$p(i) = p(i|\,|\psi\rangle) = |z_i|^2 = z_i z_i^*.$$

Let $\epsilon > 0$. We would like to know how many rounds of our experiment we need to perform—that is, how large k needs to be—in order for us to be able to *confidently* say that our empirical estimate $\tilde{p}_k(0)$ is within ϵ of the true value $p(0)$. This requires a little bit of explaining, basically having to do with the fact that $\tilde{p}_k(0)$ is itself a random variable (on the set $\{0, 1/k, 2/k, \ldots, k/k = 1\}$, but don't think too hard about this).

Let us say that we are $\delta - confident$ that our observed $\tilde{p}_k(0)$ is within ϵ if we pick k large enough so that

$$\text{Prob}(|\tilde{p}_k(0) - p(0)| \geq \epsilon) \leq \delta$$

Our goal is to find a lower bound on k (as a function of ϵ, but independent of everything else) that makes this inequality true.

To do so, we can use Chebyshev's inequality (see Appendix 1 in Nielsen and Chuang). This problem will walk you through this. The idea is exactly the same as trying to get a good estimate of the bias of an unfair coin with high confidence

(a) Let Y be the random variable on the set $\{0, 1\}$ with $p(0) = 1 - |z_0|^2$ and $p(1) = |z_0|^2$. Show that $\mathbb{E}(Y) = \mathbb{E}(Y^2) = |z_0|^2$. Use this to show the variance $\text{var}(Y) = |z_0|^2 - |z_0|^4 = |z_0|^2(1 - |z_0|^2)$.

(b) Show that $\max_{0 \leq p \leq 1} p(1-p) = 1/4$. Conclude that $var(Y) \leq 1/4$.

(c) Now let $Y_1, \ldots, Y_k$ be k i.i.d variables all having the same distribution as Y. Let X_k be the sample mean

$$\frac{1}{k}\sum_{i=1}^{k} Y_i.$$

Show that X_k is exactly the same thing as $\tilde{p}_k(0)$. (This should be very easy.)

(d) Use the fact that expectation values are linear to show $\mathbb{E}(X_k) = \mathbb{E}(\tilde{p}_k(0)) = p(0)$. (In the language of probability theory, this shows that $\tilde{p}_k(0)$ is an "unbiased estimator" of the true probability $p(0)$.)

(e) Since the Y_i are independent, the variance of their sum is the sum of their variances. Use this to show $\text{var}(X_k) = \frac{1}{k}\text{var}(Y)$.

(f) Now use Chebyshev's inequality to argue that we should take $k \geq \frac{1}{4\epsilon^2\delta}$.

(g) How big should k be if we want to be 95% confident that our estimate of $|z_0|^2$ is correct up to b bits?

Let me conclude by noting that there are better ways to do quantum state tomography!

Proof. (a) The expectation values of the random variables Y and Y^2 are, respectively,

$$\mathbb{E}(Y) = \sum_{i=1}^{2} ip(i) = (0) \cdot p(0) + (1) \cdot p(1) = |z_0|^2$$

$$\mathbb{E}\left(Y^2\right) = \sum_{i=1}^{2} i^2 p(i) = (0)^2 \cdot p(0) + (1)^2 \cdot p(1) = |z_0|^2.$$

The variance of a random variable is given by

$$\text{Var}(Y) = \mathbb{E}\left(Y^2\right) - \mathbb{E}(Y)^2 = |z_0|^2 - |z_0|^4 = |z_0|^2(1 - |z_0|^2).$$

(b) To find the maximum value for $p(1-p)$, where $p \in [0, 1]$, we can search for a maximum on that domain. Let $f(p) = p(1-p)$, then $f'(p) = 1 - 2p$. Setting $f'(p) = 0$, we get that the $p = \frac{1}{2}$. Plugging this back, we get $f\left(\frac{1}{2}\right) = \frac{1}{4}$. Thus, the maximum value for $f(p)$ is $\frac{1}{4}$ when $p = \frac{1}{2}$.

Let $p = |z_0|^2$, then $\text{Var}(Y) = p(1-p) = |z_0|^2(1 - |z_0|^2) \leq \frac{1}{4}$.

(c) We have that

$$\tilde{p}_k(0) = \frac{\#\{j | i_j = 0\}}{k}.$$

The variables Y_j and i_j are equivalent, where $i_j = 0 \iff Y_j = 1$ and $i_j \neq 1 \iff Y_j = 0$.
Then,

$$X_k = \frac{1}{k}\sum_{i=1}^{k} Y_i = \frac{\#\{i|Y_i = 1\}}{k} = \frac{\#\{j|i_j = 0\}}{k} = \tilde{p}_k(0).$$

(d) We have

$$\begin{aligned}
\mathbb{E}\left(X_k\right) &= \mathbb{E}\left(\tilde{p}_k(0)\right) \\
&= \frac{1}{k}\sum_{i=1}^{k} \mathbb{E}\left(Y_i\right) \\
&= \frac{1}{k}\sum_{i=1}^{k} |z_0|^2 \\
&= |z_0|^2 \\
&= p(0).
\end{aligned}$$

(e) We have

$$\begin{aligned}
\mathrm{Var}(X_k) &= \mathrm{Var}\left(\frac{1}{k}\sum_{i=1}^{k} Y_i\right) \\
&= \frac{1}{k^2}\mathrm{Var}\left(\sum_{i=1}^{k} Y_i\right) \\
&= \frac{1}{k^2}\sum_{i=1}^{k} \mathrm{Var}(Y_i) \\
&= \frac{1}{k^2}k\mathrm{Var}(Y) \\
&= \frac{1}{k}\mathrm{Var}(Y).
\end{aligned}$$

(f) Chebyshev's inequality states that the probability that a random variable X deviates from its mean μ by more than $k\sigma$ is at most $\frac{1}{k^2}$, where k is any positive constant and σ is the standard deviation. It is expressed as

$$P(|X - \mu| \geq k\sigma) \leq \frac{1}{k^2}.$$

We want to reach

$$\mathrm{Prob}(|\tilde{p}_k(0) - p(0)| \geq \epsilon) \leq \delta.$$

In our case, we have

$$\begin{aligned}
P\left(|X_k - \mathbb{E}\left(X_k\right)| \geq k\sigma\right) &\leq \frac{1}{k^2}, \\
P\left(|\tilde{p}_k(0) - p(0)| \geq \epsilon\right) &\leq \left(\frac{\sigma}{\epsilon}\right)^2 \qquad \left(k = \frac{\epsilon}{\sigma}\right).
\end{aligned}$$

From part (b), we have that

$$\sigma^2 = \mathrm{Var}(X_k) = \frac{1}{k}\mathrm{Var}(Y) \leq \frac{1}{4k}$$

Thus, we need

$$\begin{aligned}
\left(\frac{\sigma}{\epsilon}\right)^2 \leq \frac{1}{4k\epsilon^2} \leq \delta \\
\implies k \geq \frac{1}{4\delta\epsilon^2}.
\end{aligned}$$

(g) For a 95% confidence, we need $\delta = 0.05$, and up to b bits means we need $\epsilon = \frac{1}{2^b}$. Replacing, we get

$$k \geq \frac{1}{4(0.05)2^{-2b}} = 5 \cdot 4^b.$$

■