CSE 534 Autumn 2024: Set 2

Instructor: Chinmay Nirkhe
Due date: October 16th, 2024 10:00pm

Instructions: Solutions should be legibly handwritten or typset. Mathematically rigorous solutions are expected for all problems unless explicitly stated.

You are encouraged to collaborate on problems in small teams but everyone must individually submit solutions. Solutions for the problems may be found online or in textbooks – but do not use them.

For grading purposes, start each problem on a new page.

Problem 1 (Indistinguishable states)**.**

No need to submit a solution. When can we distinguish quantum states?

1. (**1 point**) Let $|\psi\rangle$ and $|\psi'\rangle$ be orthogonal single qubit states. Show that

$$\frac{1}{\sqrt{2}}|00\rangle + |11\rangle = \frac{1}{\sqrt{2}}|\psi, \psi^\star\rangle + \left|\psi', \psi'^\star\right\rangle. \tag{1}$$

2. (**1 point**). Let $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$. Show that the states $|\phi\rangle$ and $c|\phi\rangle$ for $c \in \mathbb{C}$ cannot be distinguished by any combination of our 'axioms of quantum computation'.
Hint: Consider the corresponding density matrices.

3. (**1 point**) Show that the following two distributions yield the same density matrix.
   (a) Flip a fair coin and set the state to be $|0\rangle$ or $|1\rangle$ depending on the outcome.
   (b) Flip a fair coin and set the state to be $|+\rangle$ or $|-\rangle$ depending on the outcome.

Only write solutions for two out of the next three problems. But solve all of them!

Problem 2 (Expectation of an operator)**.** In practice, we care about the outcome of a quantum system averaged over many trials. Consider a qubit $|\psi\rangle \in \mathbb{C}^2$ and associate the measurement $|0\rangle$ with $+1$ and a measurement of $|1\rangle$ with -1.

1. **(2 points)** Show the expectation of this experiment is $\langle\psi|Z|\psi\rangle$ where

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{2}$$

2. **(2 points)** This gives rise to the notation, $\langle Z\rangle_\psi = \langle\psi|Z|\psi\rangle$ (or $\langle Z\rangle$ when the state ψ is clear from context). Give an experiment with expectation $\langle X\rangle$ where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3}$$

3. **(1 point)** What is the appropriate definition of $\langle Z\rangle_\rho$ for a density matrix ρ? (No explanation required).

Problem 3 (Partial trace)**.**

1. **(1 point)** Consider a quantum state $\rho_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Prove that

$$\mathrm{tr}_B(\mathrm{tr}_C(\rho_{ABC})) = \mathrm{tr}_C(\mathrm{tr}_B(\rho_{ABC})) = \mathrm{tr}_{BC}(\rho_{ABC}). \tag{4}$$

2. **(2 points)** Prove that for density matrix $\sigma_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ that $\sigma_A \stackrel{\text{def}}{=} \mathrm{tr}_B(\sigma_{AB})$ is a density matrix (i.e. that it is a positive Hermitian matrix of trace 1).

3. **(2 points)** Assume $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n}$. Prove that any single-qubit standard basis measurement of σ_A has the same distribution as that obtained by measuring the same qubit of σ_{AB}.

Problem 4 (Density matrices of the W state)**.** The W_n state is an entangled state of n qubits defined as:

$$|W_n\rangle = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} \underbrace{|0\rangle \ldots |0\rangle}_{j-1 \text{ times}} |1\rangle \underbrace{|0\rangle \ldots |0\rangle}_{n-j \text{ times}} \tag{5a}$$

$$= \frac{1}{\sqrt{n}} \sum_{j=1}^{n} X_j |0^n\rangle. \tag{5b}$$

Here X_j is the X bit-flip operator applied to the j-th qubit.

1. **(2.5 points)** What is the reduced density matrix of the W state on 1 qubit?

2. **(2.5 points)** Consider the W state for $n = 3$. What is the reduced density matrix on any two of the qubits out of three?

Problem 5 (Simultaneous change of basis)**.** In this problem, we are going to prove the following statement which is very useful in characterizing the behavior of quantum devices:

For any two Hermitian operators A, B acting on a Hilbert space $\mathcal{H} \cong \mathbb{C}^d$ such that $A^2 = B^2 = \mathbb{I}$ and $AB = -BA$, there exists a change of basis U on $\mathcal{H}$ such that

$$UAU^\dagger = X \otimes \mathbb{I}_{d/2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \mathbb{I}_{d/2}, \qquad UBU^\dagger = Z \otimes \mathbb{I}_{d/2} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \mathbb{I}_{d/2} \tag{6}$$

where the $\mathbb{I}$ action is on the remaining $d/2$ dimensions. Therefore, A and B identify a decomposition of $\mathcal{H} \cong \mathbb{C}^2 \otimes \mathbb{C}^{d/2}$.

This is a challenging theorem to prove. The following setup breaks it down into manageable parts.

1. First, solve the $d = 2$ case. Meaning, you can assume that A and B are 2×2 matrices and you want to explicitly show the existence of a 2×2 unitary U such that $UAU^\dagger = X$ and $UBU^\dagger = Z$.

   (a) **(2 points)** Calculate the eigenvalues of A and B.

   (b) **(2 points)** Write B in its eigenbasis. What does $AB = -BA$ imply about A?

   (c) **(2 points)** Show the existence of a U satisfying eq. (6) in the case that $d = 2$.

2. **(2 points)** Consider matrices A and B such that there exists a unitary V such that $VAV^\dagger$ and $VBV^\dagger$ are block-diagonal with each block being a 2×2 matrix – i.e.

$$VAV^\dagger = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_{d/2} \end{pmatrix}, \quad VBV^\dagger = \begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_{d/2} \end{pmatrix}. \tag{7}$$

   Show that for such matrices, a simultaneous change of basis according to eq. (6) exists.

3. Show that eq. (7) is sufficiently general. Namely, that if general $d \times d$ Hermitian matrices exist satisfying $A^2 = B^2 = \mathbb{I}$ and $AB = -BA$, then there exists a unitary V such that eq. (7) holds.

   (a) **(2 points)** Consider any two Hermitian matrices such that $A^2 = B^2 = \mathbb{I}$ and $AB = -BA$. Let $|v\rangle$ be any eigenvector of $A + B$. Then show that both A and B preserve the eigenspace spanned by $|v\rangle$ and $AB|v\rangle$.

   (b) **(2 points)** Conclude that there exists a change of basis unitary V such that in this basis, A and B are simultaneously block-diagonal with blocks of size 1 or 2.

   (c) **(2 points)** Argue that blocks of size 1 cannot exist due to the anti-commutation condition. And therefore, we have achieved the assumption of eq. (7).

4. **(1 point)** Read the following text about what is a bit and what is a qubit. No need to write anything:

What is a bit? Given a finite vector space $V \subseteq \mathbb{F}_2^n$, we could say that V can store $k = \dim V = \log_2 |V|$ many bits of information. This is because, we can come up with a bijection between $\{0,1\}^k \longleftrightarrow V$. Ok, so there are k bits, but what are the individual bits of V?

Well, since V is a vector space, we can find a basis $v_1, \ldots, v_k$ for V and write the matrix

$$M = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_k \\ | & & | \end{pmatrix}. \tag{8}$$

This helps us make the bijection between $\{0,1\}^k \longleftrightarrow V$ with x mapping to Mx. In which case, the set of strings with the 1st bit equaling 0 would be $V_0 \stackrel{\text{def}}{=} \{Mx \mid x_1 = 0\}$ and, likewise, the set of strings with the 1st bit equaling 0 would be $V_1 \stackrel{\text{def}}{=} \{Mx \mid x_1 = 1\}$.

This gives us the natural interpretation of the "bit-flip" of the first bit as adding the vector v_1. Likewise, we can define each of the bits by their corresponding "bit-flip" v_i. In a technical sense, it is precisely these k bit-flips that define why and how V encodes k bits. A key property is that "flipping" the first bit does not change the value of the other encoded bits. In this technical sense, the k bits we have identified are truly independent.

But it important to note that we only "found" the bits because we chose $v_1, \ldots, v_k$ as a basis for V. This is not the only basis we could have chosen and each basis given a different interpretion of the bits of V. This is why we might say that the "bits are in the eye of the beholder" because the basis that V is being interpreted in matters. A particularly important instance of this phenomenon is when V is the codespace of a binary linear code. In which case, the vectors $v_1, \ldots, v_k$ are the logical bit-flips of the code.

What is a qubit? A similar phenomenon occurs when we study qubits. Intuitively, we want that our notion of separate qubits has the property that single-qubit operators do not change the information expressed in the other qubits.

The theorem we proved showed that a single pair of anti-commuting observables[1] give a decomposition of the Hilbert space into a tensor product of a two-dimensional space where the operators act non-trivially and the remainder of the space where the operators act trivially. Therefore, if we were to find a collection of observables $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ so that all of them commuted except A_i and B_i anticommuted, then we could iteratively apply the theorem to decompose the Hilbert space into a tensor product of two-dimensional spaces such that A_i and B_i act non-trivially on the i-th identified subspace and all other matrices act trivially on the i-th subspace.

Therefore this is the "qubit is in the eye of the beholder" analog of the classical statement – namely that the qubit is fundamentally defined by its bit (X) and phase (Z) flips. The state in the Hilbert space depends on the basis in which it is being observed and the basis is precisely defined by the bit and phase flips we identify. We speak about this very loosely here, but this can be made highly rigorous.

This perspective turns out to be incredibly useful for understanding quantum error correction, non-local games, and certain cryptographic schemes. And the best part is that the mathematics of it, albeit daunting at first, is understandble by most!

Problem 6. Consider a device that ideally produces the state $|\psi_0\rangle$ but due to manufacturing defects produces the state $|\psi_1\rangle$. We will show that if $|\psi_0\rangle$ and $|\psi_1\rangle$ have large overlap $|\langle\psi_0|\psi_1\rangle|$, then no quantum process can distinguish these two devices with high probability. For any process P, quantify how well it distinguishes $|\psi_0\rangle$ and $|\psi_1\rangle$ by:

$$\Delta \stackrel{\text{def}}{=} \left|\mathbf{Pr}(P(|\psi\rangle_0) \text{ outputs } 0) - \mathbf{Pr}(P(|\psi\rangle_1) \text{ outputs } 0)\right| \tag{9}$$

[1] An observable, for our context, will be any Hermitian operator that squares to identity.

1. **(2 points)** Consider the simplest strategy: measure in a basis for which $|\psi_0\rangle$ is a basis vector and guess 0 if the measurement is $|\psi_0\rangle$ and 1 otherwise. Show that then

$$\Delta = 1 - |\langle\psi_0|\psi_1\rangle|^2. \tag{10}$$

2. **(2 points)** This strategy is not optimal. Find a better measurement for which

$$\Delta = \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}. \tag{11}$$

   (Hint: There is a 2-dimensional space containing $|\psi_0\rangle$ and $|\psi_1\rangle$. It may be useful to remember the trignometric identities of $2\sin x \sin y = \cos(x-y) - \cos(x+y)$ and $\cos 2x = 2\cos^2 x - 1$.)

We will show that this second strategy is indeed optimal. To show the upper bound of eq. (11), we will first introduce a generalized form of measurement called a *positive-operator valued measurement* (POVM). A POVM is a set of Hermitian positive semidefinite operators $\{M_i\}$ on a Hilbert space $\mathcal{H}$ that sum up to identity

$$\sum_{i=1}^{n} M_i = \mathbb{I}_{\mathcal{H}}. \tag{12}$$

The probability of measuring outcome i is given by $\mathbf{Pr}(i) = \langle\psi|M_i|\psi\rangle$. This generalizes a basis measurement as we can consider $M_i = |b_i\rangle\langle b_i|$ for any basis $\{|b_i\rangle\}$. An important difference between basis measurements and POVMs are that the element of a POVM are not necessarily orthogonal and, therefore, the number of elements can be larger than the dimension of the Hilbert space $\mathcal{H}$.

Instead, POVMs are exactly as descriptive as as applying a unitary U to the state and ancilla $|\psi\rangle \otimes |0\ldots0\rangle$ followed by a measurement of some of the qubits.

3. **(2 points)** For any POVM $\{M_i\}$, let $A_i = \sqrt{M_i}$, consider the following partial transformation:

$$U : |\psi\rangle|0\rangle_{\mathsf{ancilla}} \mapsto \sum_{i=1}^{n} A_i|\psi\rangle|i\rangle_{\mathsf{ancilla}}. \tag{13}$$

   Conclude that U followed by a measurement of the ancilla register gives the same statistics as the POVM.

4. **(2 points)** Given a unitary U acting on the state and some ancilla of dimension n initialized to zero, construct a POVM equivalent to applying U and measuring the ancilla in the standard basis.

Returning to the problem at hand, we can generalize the distinguishing measurement as a POVM with two elements M and $\mathbb{I} - M$, with the two outcomes corresponding to answering 0 and 1, respectively. Attempt the next four parts if you are able to – if not, you will get another chance to return to them when we will have covered some more background material in class.

5. **(2 points)** Show that then the optimal value of Δ is

$$\Delta_{\text{opt}} = \max_{0 \leq M \leq \mathbb{I}} \text{tr}\,(M\rho) \tag{14}$$

where $\rho = |\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|$.

6. **(2 points)** Conclude that

$$\max_{0 \leq M \leq \mathbb{I}} \text{tr}\,(M\rho) = \frac{1}{2}\,\text{tr}\,\sqrt{\rho^2}. \tag{15}$$

(Hint: Consider an optimal M in the basis where ρ is diagonal).

7. **(2 points)** Finish by showing

$$\text{tr}\,\sqrt{\rho^2} = 2\sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}. \tag{16}$$

(Hint: ρ is a rank 2 matrix; therefore it has only 2 non-zero eigenvalues. Now express $\text{tr}\left(\rho^2\right)$ in two ways.)

8. **(1 point)** Give a justification as to why the maximizing M and the measurement you gave in Part 2 are the same.