CSE 534 Autumn 2025: Set 2

Instructor: Chinmay Nirkhe
Due date: October 16th, 2025 11:59pm

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

You are encouraged to collaborate on problems in small teams; however, each team member must write and submit their own individual solution. Read the AI tools policy on the course webpage. Furthermore, 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)**.** When can we distinguish quantum states? **This problem is not graded. Do not submit a solution, but do solve the problem.**

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

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

2. 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. 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 one 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

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

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

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

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

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

2. **(2 points)** Prove that for density matrix $\sigma_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ that $\sigma_A \overset{\text{def}}{=} \mathrm{tr}_B(\sigma_{AB})$ 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:

$$\begin{aligned} |W_n\rangle &= \frac{1}{\sqrt{n}} \sum_{j=1}^{n} \underbrace{|0\rangle \ldots |0\rangle}_{j-1 \text{ times}} |1\rangle \underbrace{|0\rangle \ldots |0\rangle}_{n-j \text{ times}} \\ &= \frac{1}{\sqrt{n}} \sum_{j=1}^{n} X_j |0^n\rangle . \end{aligned}$$

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

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

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

The following setup breaks down the proof into manageable parts.

However, you can prove it any which way you like!

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. (1) 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.

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

   Show that for such matrices, a simultaneous change of basis according to eq. (1) exists.

3. Show that eq. (2) 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. (2) 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 vector space 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. (2).

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:

$$\Delta \stackrel{\text{def}}{=} |\mathbf{Pr}(P(|\psi_0\rangle) \text{ outputs } 0) - \mathbf{Pr}(P(|\psi_1\rangle) \text{ outputs } 0)|.$$

Solve the first two parts of this problem individually.

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

$$\Delta = 1 - |\langle\psi_0|\psi_1\rangle|^2.$$

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

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

(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, 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

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

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:

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

Conclude that U is a unitary and that if U is followed by a measurement of the ancilla register, this produces 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

$$\Delta_{\text{opt}} = \max_{0 \le M \le \mathbb{I}} \operatorname{tr}(M\rho)$$

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

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

$$\max_{0 \le M \le \mathbb{I}} \operatorname{tr}(M\rho) = \frac{1}{2} \operatorname{tr} \sqrt{\rho^2}.$$

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

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

$$\operatorname{tr} \sqrt{\rho^2} = 2\sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}.$$

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

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

Problem 7 (Alice, Bob, and Bob play CHSH)**.** The CHSH game is described as a game between non-communicating Alice and Bob where Alice receives an input bit x, Bob receives an input bit y, and they answer with bits a and b, respectively, such that $a \oplus b = xy$.

Consider the following game between non-communicating Alice, Bob_1, and Bob_2: The referee first flips a coin $i \in \{1, 2\}$ and then sends Alice an input bit x, and sends Bob_i the input bit y, and they answer with bits a, b, respectively. The other Bob neither receives a question nor answers. The winning conditioning is still $a \oplus b = xy$.

(6 points) Prove that there exists a $\delta > 0$, such that any quantum strategy succeeds with probability $\le \cos^2(\pi/8) - \delta$. For half-credit, prove that no quantum strategy wins with probability $= \cos^2(\pi/8)$. **If this problem is challenging for you, relax and submit it with the next problem set.**