CSE 534 Autumn 2025: Set 3

Instructor: Chinmay Nirkhe
Due date: November 6th, 2025 11:59pm

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; 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 (Distance measures for states)**.** The space of n-qubits, $(\mathbb{C}^2)^{\otimes n}$, is a Hilbert space meaning it is a vector space imbibed with an inner product. In this case, the inner product between vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ is simply $\langle\psi_1|\psi_2\rangle$. This gives us a notion of distance for unit vectors, by

$$\||\psi_1\rangle - |\psi_2\rangle\| = \sqrt{2 - 2\,\mathrm{Re}\,\langle\psi_1|\psi_2\rangle}. \tag{1}$$

1. **(2 points)** Show that whenever the norm is $\leq \epsilon$, the success probability of any distinguishing measurement is at most ϵ. (You can use the previous problems set's solution).

2. **(2 points)** Is the converse true? Does the distinguishing probability being small imply the norm is small? Give a counterexample or a proof.

3. **(2 points)** Turns out there is a convenient measure for distance between density matrices. To define it, we first define an inner product over square matrices:

$$\langle\rho, \sigma\rangle \stackrel{\text{def}}{=} \mathrm{tr}\left(\sqrt{\rho^\dagger \sigma}\right). \tag{2}$$

   This inner product yields a norm $\|\rho\|_1$ called the trace norm. What is the value of this norm when ρ is a Hermitian matrix?

4. **(2 points)** Find an expression for $\||\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2|\|_1$ relating it to the optimal distinguishing measurement probability. (Use previous parts or problems from previous sets. Don't reinvent the wheel, please.)

5. **(2 points)** Let's generalize. Compute the optimal distinguishing probability for distinguishing density matrices ρ_1 and ρ_2. Use the same techniques as steps 5-8 of the previous problem set.

Problem 2. Let ρ be a density matrix and $\{\Pi, \mathbb{I} - \Pi\}$ be a POVM such that $\mathrm{tr}(\Pi\rho) \geq 1 - \epsilon$. Let ρ' be the post-measurement state.

1. **(2 points)** State and prove an upper bound on $\|\rho - \rho'\|$.

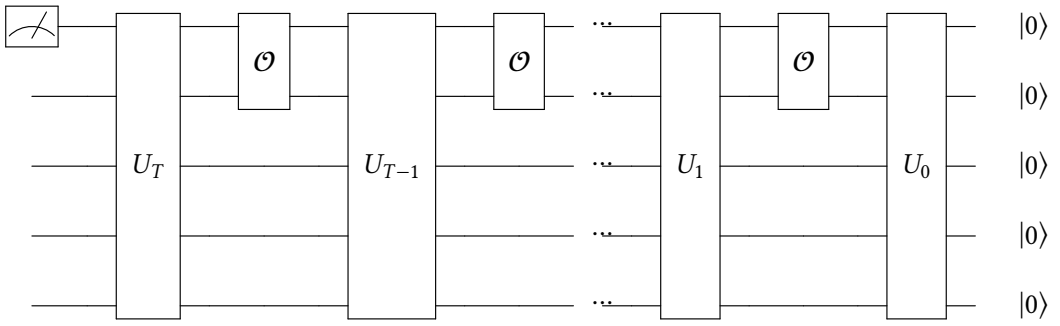
2. **(1 point)** Argue by constructing an example that the upper bound is tight.

Problem 3. (2 points) Let ρ and σ be two density matrices $\in \mathcal{H}_A \otimes \mathcal{H}_B$. Prove that

$$\|\mathrm{tr}_A(\rho) - \mathrm{tr}_A(\sigma)\|_1 \leq \|\rho - \sigma\|_1. \tag{3}$$

Problem 4 (Quantum query lower bounds)**.** In class, we saw a proof that of the famous Bennett, Bernstein, Brassard, and Vazirani (BBBV) 1994 result that showed that any quantum query algorithm that succeeds in solving unconstrained search over a set of size N requires $\Omega(\sqrt{N})$ queries. In this problem, you will prove one such generalization which can be used to lower bound the query complexity of more general oracle problems.

Recall the setup: A quantum query algorithm access a classical boolean string $\mathbf{x}$ of length $N = 2^n$ with gates of the form: $|i\rangle \mapsto (-1)^{x_i} |i\rangle$ for $i \in \{1, \ldots, N\}$. The queries to the string $\mathbf{x}$ are interspersed with quantum computations that are independent of $\mathbf{x}$. A generic quantum query algorithm with T queries can be expressed as the following circuit[1]:



Here the large gates $U_0, U_1, \ldots, U_T$ are meant to represent quantum circuits of poly(n) gates acting on at most $m = \mathrm{poly}(n)$ qubits; however, we will only assume they to be unitaries. The gates $\mathcal{O}$ are defined as the linear extensions of $|i\rangle \mapsto (-1)^{x_i} |i\rangle$ for $i \in \{1, \ldots, N\}$. They are also known as "oracle" gates.

1. **(1 point)** True or False: If we prove a quantum query lower bound only assuming that U_t are unitaries, this is weaker than assuming that U_t are poly(n) sized quantum circuits. (No explanation required.)

[1] Require our convention of circuits running from right to left.

Notice that the input "kets" to the quantum query algorithm is all zeroes. We will now manipulate this generic format. Consider a larger input of $|0 \dots 0\rangle \otimes |\mathbf{x}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_I$ where $\mathcal{H}_A$ was the original Hilbert space and $\mathcal{H}_I \equiv \mathbb{C}^N$ is an additional Hilbert space we append. Next, every oracle gate is converted to include an action on $\mathcal{H}_I$ defined by

$$|i, \mathbf{x}\rangle \mapsto (-1)^{x_i} |i, \mathbf{x}\rangle . \tag{4}$$

2. **(1 point)** Draw a new quantum circuit diagram for this adjusted picture.

Mathematically, the two quantum circuits compute the exact same state over $\mathcal{H}_A$. The leverage of this setup is that we can "run" the quantum query algorithm in *superposition* over inputs $\mathbf{x}$. It is important to observe that this is purely hypothetical but sufficient for proving the lower bound.

To setup a decision problem, we need a set of strings that we will accept and a set of strings we will reject. We call these YES and NO, respectively. A query algorithm $\mathcal{A}$ decides the task with error $\epsilon > 0$, if

$$\forall\, \mathbf{y} \in \mathsf{YES}, \quad \Pr_{\mathcal{A}} [\mathcal{A}^{\mathbf{y}} \text{ accepts}] \geq 1 - \epsilon \tag{5a}$$

$$\forall\, \mathbf{x} \in \mathsf{NO}, \quad \Pr_{\mathcal{A}} [\mathcal{A}^{\mathbf{x}} \text{ accepts}] \leq \epsilon. \tag{5b}$$

Assume we have an algorithm $\mathcal{A}$ which decides the task with error $\epsilon < \frac{1}{2}$ using T queries. We are going to prove a lower bound on T. As previously suggested, we are going to run the quantum query algorithm with the register $\mathcal{H}_I$ initially set to the following state:

$$|\chi_0\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2|\mathsf{YES}|}} \sum_{\mathbf{y} \in \mathsf{YES}} |\mathbf{y}\rangle + \frac{1}{\sqrt{2|\mathsf{NO}|}} \sum_{\mathbf{z} \in \mathsf{NO}} |\mathbf{z}\rangle . \tag{6}$$

Define $|\Psi_t\rangle$ to be the state immediately after applying the unitary U_t starting with $|0\rangle \otimes |\chi_0\rangle$. Define $\rho_t \stackrel{\text{def}}{=} \mathrm{tr}_{\mathcal{H}_A} (|\Psi_t\rangle\langle\Psi_t|)$, the reduced density matrix on $\mathcal{H}_I$.

3. **(2 points)** Prove that

$$(\rho_0)_{\mathbf{yz}} = \frac{1}{2\sqrt{|\mathsf{YES}| \cdot |\mathsf{NO}|}}. \tag{7}$$

4. **(2 points)** Let $|\psi_{\mathbf{x}}\rangle$ be the output quantum state before the measurement when the oracle is fixed to $|\mathbf{x}\rangle$. Express $|\Psi_T\rangle$ in terms of $\{|\psi_{\mathbf{y}}\rangle\}_{\mathbf{y} \in \mathsf{YES}}$ and $\{|\psi_{\mathbf{z}}\rangle\}_{\mathbf{z} \in \mathsf{NO}}$.

5. **(3 points)** Prove that

$$(\rho_T)_{\mathbf{yz}} \leq \frac{\sqrt{\epsilon(1-\epsilon)}}{\sqrt{|\mathsf{YES}| \cdot |\mathsf{NO}|}}. \tag{8}$$

Hint: express $|\psi_{\mathbf{y}}\rangle$ and $|\psi_{\mathbf{z}}\rangle$ as $\sum_{b,u} \alpha_{bu} |b\rangle |u\rangle$ with $|b\rangle$ identify the measurement qubit.

6. **(1 point)** Define $S_t \stackrel{\text{def}}{=} \sum_{\mathbf{y}\in\mathsf{YES},\mathbf{z}\in\mathsf{NO}} \left|(\rho_t)_{\mathbf{yz}}\right|$. Show that if $S_t - S_{t+1} \le \delta$ for all $t = 0, \ldots, T-1$, then

$$T \ge \left(\frac{1}{2} - \sqrt{\epsilon(1-\epsilon)}\right)\frac{\sqrt{|\mathsf{YES}|\cdot|\mathsf{NO}|}}{\delta}. \tag{9}$$

Therefore, a technique for proving lower bounds on query complexity is to argue that δ is not too large. Notice that up till now, we have not used any structure of the sets YES and NO other than their cardinality. Next, we will come up with one setting where we can bound δ. Define

$$\ell_{\mathbf{y},i} \stackrel{\text{def}}{=} \#\{\mathbf{z}\in\mathsf{NO} : z_i \neq y_i\}, \tag{10a}$$

$$\ell'_{\mathbf{z},i} \stackrel{\text{def}}{=} \#\{\mathbf{y}\in\mathsf{YES} : y_i \neq z_i\}, \tag{10b}$$

$$L \stackrel{\text{def}}{=} \max_{i=1,\ldots,N} \max_{\substack{\mathbf{y}\in\mathsf{YES},\ \mathbf{z}\in\mathsf{NO}\\ x_i\neq y_i}} \ell_{\mathbf{y},i}\ell'_{\mathbf{z},i} \tag{10c}$$

We will end up showing that $\delta = \sqrt{L}$ is one such bound.

7. **(1 point)** Without loss of generality, show that we can write the state $|\Psi_t\rangle$ as

$$|\Psi_t\rangle = \sum_{i,v} \sqrt{p_{iv}}\,|i,v\rangle_A \otimes |\zeta_{iv}\rangle_I \quad \text{where} \quad |\zeta_{iv}\rangle_I = \sum_{\mathbf{x}} \alpha_{i,v,\mathbf{x}}\,|x\rangle_I \text{ is a state of unit norm} \tag{11}$$

and $|i\rangle$ is the state that the oracle acts on and $|v\rangle$ is the remainder state of the computation.

8. **(1 point)** Show that we can express the state after the oracle query as

$$\mathcal{O}\,|\Psi_t\rangle = \sum_{i,v} \sqrt{p_{iv}}\,|i,v\rangle_A \otimes |\zeta'_{iv}\rangle_I\,. \tag{12}$$

What is $|\zeta'_{iv}\rangle_I$?

9. **(3 points)** Notationally, let $\zeta_{iv} = |\zeta_{iv}\rangle\langle\zeta_{iv}|$ and $\zeta'_{iv} = |\zeta'_{iv}\rangle\langle\zeta'_{iv}|$, be the corresponding density matrices. Show for all i, v, that

$$S_{i,v} \stackrel{\text{def}}{=} \sum_{\mathbf{y}\in\mathsf{YES},\mathbf{z}\in\mathsf{NO}} \left|(\zeta_{iv})_{\mathbf{yz}} - (\zeta'_{iv})_{\mathbf{yz}}\right| \tag{13}$$

is at most $\sqrt{L}$.

Hint: Use the AM-GM inequality in a clever manner.

10. **(2 points)** Express $\rho_t \stackrel{\text{def}}{=} \mathrm{tr}_{\mathcal{H}_A}(|\Psi_t\rangle\langle\Psi_t|)$ and ρ_{t+1} in terms of $\{p_{iv}\}$, $\{\zeta_{iv}\}$, $\{\zeta'_{iv}\}$.

11. **(2 points)** Prove that $S_t - S_{t+1} \le \sqrt{L}$, where S_t was defined earlier.

12. **(1 point)** Put it all together and argue that any query algorithm $\mathcal{A}$ solving this problem requires at least T queries where

$$T = \left(\frac{1}{2} - \sqrt{\epsilon(1-\epsilon)}\right)\sqrt{\frac{|\mathsf{YES}| \cdot |\mathsf{NO}|}{L}}. \tag{14}$$

Problem 5 (Applying the query lower bound)**.**
Solve this problem individually. (4 points) Using the previous method, argue a query lower bound for any quantum query algorithm distinguishing oracles $\mathcal{O} : [N] \to \{0,1\}$ of Hamming weight N^α from oracles $\mathcal{O}'$ of Hamming weight N^β. Assume that $0 < \alpha < \beta < 1$.

Problem 6 (Understanding Grover's)**.**

1. **(2 points)** Give a circuit for running Grover's search on 2 qubits where $f(x) = 1$ for exactly one $x \in \{0,1\}^2$. What is the optimal number of Grover iterations needed and what is the probability of finding x?

2. **(4 points)** Consider an f where there is a unique solution $x^\star$ to $f(x) = 1$ for $x \in \{0,1\}^n$. What happens if someone impatiently runs Grover's search by measuring the state of the quantum algorithm between each iteration of Grover's search to see if it has found a solution yet? Formally, between each Grover iteration, they measure according to the following POVM:

$$\left\{ M_0 = \sum_{x\,:\,f(x)=0} |x\rangle\langle x|, M_1 = |x^\star\rangle\langle x^\star| \right\}.$$

   What is the expected number of Grover iterations till the measurement $\{M_0, M_1\}$ outputs $x^\star$?

3. **(2 points)** In class, we discussed, but did not prove, that Grover's search for finding some solution $x \in \{0,1\}^n$ when promised there are K solutions runs in time $\sqrt{2^n/K}$. Prove this statement. (No need to repeat the proof of Grover's from class. Just note the few lines where it will differ.)

4. **(2 points)** Consider running your modified Grover's search algorithm for K solutions when there are actually K' solutions. What is the probability that it will output a solution?

5. **(2 points)** Come up with a Grover's search algorithm for finding a solution $x \in \{0,1\}^n$ when the number of solutions is unknown. What is the runtime? If your algorithm is not deterministic, express the runtime in terms of N and δ, the probability of not outputting a solution.

Problem 7 (Odd cycle game)**.** Alice and Bob approach you claiming that they can 2 color any n-cycle for odd n. Amazed at this remark, you ask them to show you their solution. Having a proprietary solution$^{\text{TM}}$ to the problem, they don't want to reveal the full coloring, but they agree to the following game: Alice and Bob

will be put in separate rooms (with no communication possible between them), and you can prompt each of them with a vertex $v \in [n]$ and the will respond with $c(v)$, the purported color of v.

You agree and setup the following game: with half probability, you ask Alice and Bob about the same uniformly random vertex $v \in [n]$, and check that Alice's answer $a \in \{0,1\}$ matches that of Bob's answer $b \in \{0,1\}$. And with half probability, you ask Alice about a uniformly random v and Bob about $(v+1) \pmod n$, and check that $a \neq b$.

1. **(2 points)** Calculate the optimal classical value of the game when n is odd.

2. **(4 points)** What about the optimal quantum value to the game? Recall our in-class exploration of the CHSH game. We can characterize Alice's strategy by an observable $\{A_v\}$ for every $v \in [n]$ and Bob's strategy by an observable $\{B_v\}$ for every $v \in [n]$ with a shared state $|\psi\rangle_{AB}$. Construct a quantum strategy that achieves a success probability of at least $1 - \frac{\pi^2}{8n^2}$.
   Hint: They only need to share an EPR pair.

3. **(2 points (bonus))** Can you improve your previous strategy to get a success probability of at least $1 - \frac{\pi^2}{16n^2}$? Show how.

4. **(2 points)** Do you think that the quantum value of the odd-cycle game is 1? Give an intuitive argument why or why not (no need for a rigorous proof). You can assume that the optimal strategy for Alice and Bob is to hold a maximally entangled state of dimension d: $\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_B$ — this state is equal to the tensor product of m EPR pairs when $d = 2^m$.