Name: Dakshita

UID: 123456

CS 498 QC Fall 2023 – Final Exam

Due Tuesday, November 28, 4:45 pm

- Please write your name and UID in the spaces provided and attach this sheet to the front of your solutions. **No collaboration is allowed in this exam. Any collaboration or discussion or looking at sources outside the recommended course textbook will be considered a violation of the student code, and may result in suspension from UIUC.**
- Please write your answers in a neat and readable hand-writing. Each answer should be on a separate page. *There are plenty of extra spaces, you do not need to fill them all. You should expect answers to be fairly short.*
- Always explain your answers, unless you're explicitly told that no explanation is necessary. All the best!

Honor Code (READ CAREFULLY). I agree to follow the rules stated below:

- I am not allowed to collaborate with anyone, including my fellow UIUC students, when answering this exam. I will work on this exam entirely on my own and without the help of any other person or any other student's notes or solutions.
- I will not seek out or make use of any outside source of information, including information found in books or notes or on the internet.
- **I understand that I may be suspended from UIUC for violating this honor code.**
- If I have difficulty understanding any question in the exam due to difficulty with the English language or otherwise, I will talk to the professor for clarification and will ensure that the honor code is upheld.
- I will follow these rules in good faith, and not try to find "loopholes" that violate the spirit of the rules. If I am unsure about what the spirit of the rule is or what a rule means, then I will ask the professor for clarification, and I will adhere to rules as clarified.

Note: This exam has a total of 5 questions, for a total of 30 points.

1. **TRUE OR FALSE (6 points). Write whether the following statements are true or false. Explain your answer in one line.**

   (a) By using classical strategies, Alice and Bob can win the CHSH game with probability at most 3/8.

   FALSE. There is a classical strategy that wins CHSH w.p. 3/4.

   (b) For every density matrix, there is a unique probabilistic mixture of pure states that the density matrix represents.

   FALSE. The states $\{\frac{1}{2}|0\rangle, \frac{1}{2}|1\rangle\}$ and $\{\frac{1}{2}|+\rangle, \frac{1}{2}|-\rangle\}$ have the same density matrix.

   (c) In QKD, if Eve knows only that some particular qubit is either $|+\rangle$ or $|-\rangle$, she cannot learn which without altering the qubit.

   FALSE. A Hadamard basis msmt reveals if it is $|+\rangle$ or $|-\rangle$ without disturbing the qubit.

   (d) Quantum computers are known to solve NP-hard problems in polynomial time by trying out all (exponentially many) solutions in superposition.

   FALSE. This is not known, lower bounds in the query model indicate that quantum comps need subexponential time.

   (e) The error-correcting code that maps $|0\rangle \mapsto |000\rangle$ and $|1\rangle \mapsto |111\rangle$ can correct arbitrary phase flip errors on a single qubit.

   FALSE. The code $|0\rangle \to |000\rangle$ and $|1\rangle \to |111\rangle$ can correct bit flip errors but cannot recover from phase flip errors.

   (f) Quantum computers can simulate arbitrary Hamiltonians, that is, starting with initial n-qubit state $|\psi_0\rangle$, approximate the time-evolved state $e^{iHt}|\psi_0\rangle$ for arbitrary $2^n \times 2^n$ matrix H in polynomial time.

   FALSE. Only known quantum polytime algorithms for this task apply when H is a LOCAL Hamiltonian

2. **MAJORITY (6 points).** The 3-bit majority function MAJ : $\{0,1\}^3 \to \{0,1\}$ takes value 1 iff at least 2 of its 3 inputs bits are 1.

   (a) **(4 points).** A box hides bitstring $a = a_1a_2a_3 \in \{0,1\}^3$. You can query the box on input location i to obtain a_i, i.e. a query applies the unitary $|i,b\rangle \mapsto |i, b \oplus a_i\rangle$.
   Give a quantum algorithm that computes MAJ(a) with success probability 1 (for every possibility of $a \in \{0,1\}^3$), **using only 2 queries** to the box.

$|1,0\rangle \to |1,a_1\rangle$

$|2,0\rangle \to |2,a_2\rangle$

$|3,0\rangle \to |3,a_3\rangle$

$\frac{1}{\sqrt{2}}\left(|1,-\rangle + |2,-\rangle \right)$

↓ query the box

$\frac{1}{\sqrt{2}}\left((-1)^{a_1}|1,-\rangle + (-1)^{a_2}|2,-\rangle \right)$

If $a_1 = a_2$: this is $\frac{1}{\sqrt{2}}\left(|1\rangle + |2\rangle \right) \otimes |-\rangle = |+\rangle \otimes |-\rangle$

$a_1 \neq a_2$: this is $\frac{1}{\sqrt{2}}\left(|1\rangle - |2\rangle \right) \otimes |-\rangle = |-\rangle \otimes |-\rangle$

If $a_1 = a_2$ (msmnt returned "+"), then query again to find a_1 and output it.

If $a_1 \neq a_2$ query to find a_3 and output it.

(b) **(2 points).** How many quantum queries would you need to compute MAJ if you allow an algorithm to have error probability at most $1/3$ on every input? Explain your answer.

$a_1 a_2 a_3 = 0\ 1\ 1$

$\left(|1, a_1\rangle + |2, a_2\rangle + |3, a_3\rangle \right)$

Sample $i \leftarrow \{1, 2, 3\}$

Obtain a_i with a single classical query

output a_i.

$\Pr[$ A single random query returns $MAJ(a_1 a_2 a_3)]$

$\geq \frac{2}{3}$.

3. **ENTANGLEMENT (9 points).** Alice and Bob share n EPR pairs. Call their shared 2n-qubit state $|\psi\rangle_{AB}$.

   (a) **(3 points.)** Let U be an arbitrary n-qubit unitary and $\overline{U}$ be U after conjugating its entries (without transposing). Prove that $(U \otimes \overline{U})\,|\psi\rangle_{AB} = |\psi\rangle_{AB}$.

$$|\psi\rangle_{AB} = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes n}$$

$$= \frac{1}{2^{n/2}} \sum_{j \in \{0,1\}^n} |jj\rangle_{AB}$$

$$(U \otimes \bar{U}) \frac{1}{2^{n/2}} \sum_{j \in \{0,1\}^n} |jj\rangle_{AB}$$

$$= \frac{1}{2^{n/2}} \sum_{j \in \{0,1\}^n} \left(\sum_{\substack{i \in \{0,1\}^n \\ k \in \{0,1\}^n}} U_{ij} \, U^*_{kj} \, |i\rangle|k\rangle \right)$$

$= 0$ when $|i\rangle \neq |k\rangle$ (U is unitary, so its rows are orthonormal)

$= 1$ when $|i\rangle = |k\rangle$

$$= \frac{1}{2^{n/2}} \sum |i\rangle|i\rangle = |\psi\rangle_{AB}.$$

(b) **(3 points.)** Suppose Alice receives some input x, and she applies an n-qubit unitary U_x on her part of the state and then measures in the computational basis, obtaining a classical outcome $a \in \{0,1\}^n$. What is the probability distribution over Alice's measurement outcomes, and why?

$(U_x \otimes \mathbb{I})|\psi_{AB}\rangle$

Alice's density matrix is $\frac{\mathbb{I}}{2^n}$

After applying U_x, this becomes

$$U_x \frac{\mathbb{I}}{2^n} U_x^\dagger$$

$$= \frac{U_x U_x^\dagger}{2^n} = \frac{\mathbb{I}}{2^n}.$$

Thus, Alice's outcomes are uniformly distributed.

(c) **(3 points.)** Suppose Bob receives the same input x as Alice already received. How can he learn Alice's measurement outcome a without communication?

Because Alice applied U_x,

Bob should apply $\overline{U}_x$.

By (a), we know

$$(U_x \otimes \overline{U}_x)|\psi\rangle_{AB} = |\psi\rangle_{AB}.$$

$\Rightarrow$ Bob's outcome will match Alice's measurement outcome in the computational basis.

4. **PARALLELIZING SEARCH (5 points).** This question is about parallelizing search.

Let $p \geq 1$ be a fixed integer. Suppose you have a function $f : \{0,1\}^n \to \{0,1\}$ and you have a special kind of oracle Q_f that answers p binary queries to f in parallel:

$$Q_f : |x_1, b_1, x_2, b_2, \ldots, x_p, b_p\rangle \mapsto |x_1, b_1 \oplus f(x_1), x_2, b_2 \oplus f(x_2), \ldots, x_p, b_p \oplus f(x_p)\rangle$$

where the x_j's are in N for $N = 2^n$ and the b_j's are bits.

Show how you can find a solution to the search problem (i.e., an $x \in \{0,1\}^n$ such that $f(x) = 1$, given that one such x exists) using $O(\sqrt{N/p})$ applications of Q_f. You may assume for simplicity that N/p is a power of 2. A precise higher-level description suffices, no need to draw a circuit.

Trivial Grover: N entries, $\sqrt{N}$ queries

$\frac{N}{p}$ entries?, $\sqrt{\frac{N}{p}}$ queries

$Q_f : |x_1, b_1, x_2, b_2\rangle \to |x_1, b_1 \oplus f(x_1), x_2, b_2 \oplus f(x_2)\rangle$

Split $\{0,1\}^n$ into p sets, each of size $\frac{N}{p}$

$\text{Set}_1 = [1 \ldots \frac{N}{p}]$, $\text{Set}_2 = [\frac{N}{p}+1 \ldots \frac{2N}{p}]$, $\text{Set}_3 = [\frac{2N}{p}+1 \ldots \frac{3N}{p}]$

$\text{Set}_p = [\frac{(p-1)N}{p}+1 \ldots N]$

Prepare state $\sum_{x_1 \in \text{Set}_1} |x_1, -\rangle \sum_{x_2 \in \text{Set}_2} |x_2, -\rangle \ldots \sum_{x_p \in \text{Set}_p} |x_p, -\rangle$

(Extra page for solutions)

Query Q_f to obtain

$$\underbrace{\sum_{x_1 \in \text{Set}_1} (-1)^{f(x_1)} |x_1, -\rangle}_{x_1 \in \text{Set}_1} \cdots \underbrace{\sum_{x_p \in \text{Set}} (-1)^{f(x_p)} |x_p, -\rangle}_{x_p \in \text{Set}}$$

Perform the "inversion about mean step"

by applying unitary $U \otimes U \otimes \cdots \otimes U$ (p times)

where $U = 2|+\rangle\langle+| - \mathbb{I}$

Repeat $\sqrt{N/p}$ times

Each parallel session gives a candidate solution.

Call these $y_1 \cdots y_p$.

Query on $|y_1, 0\rangle, |y_2, 0\rangle \cdots |y_p, 0\rangle$

$\downarrow$

$|y_1, f(y_1)\rangle, |y_2, f(y_2)\rangle \cdots |y_p, f(y_p)\rangle$

One of these should be a solution.

5. **MISCELLANEOUS (4 points).**

(a) **(2 points).** What are the eigenvectors and eigenvalues of the 1-qubit unitary

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

$|X - \lambda I| = 0 \Rightarrow \left| \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right| = 0$

$\Rightarrow \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = 0 \Rightarrow \lambda^2 - 1 = 0$

$\Rightarrow \lambda = \pm 1$

$|+\rangle$

$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = 1 \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \Rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \Rightarrow \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

$\Rightarrow \beta = \alpha$

$X \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = -1 \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \Rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} -\alpha' \\ -\beta' \end{bmatrix} \Rightarrow \begin{bmatrix} \beta' \\ \alpha' \end{bmatrix} = \begin{bmatrix} -\alpha' \\ -\beta' \end{bmatrix}$

$\Rightarrow \beta' = -\alpha'$

$|-\rangle$

So the two eigenvalues are $+1$ and -1 with eigenvectors $|+\rangle$ and $|-\rangle$ respectively.

(b) **(2 points).** Let $|\psi\rangle$ be an arbitrary single-qubit state. Show that the mixed state obtained by sampling $x \leftarrow \{0,1\}, z \leftarrow \{0,1\}$ and outputting $X^x Z^z |\psi\rangle$ is the maximally mixed state.

$X^x Z^z |\psi\rangle = |\psi\rangle$ when $x=0, z=0$

$X^x Z^z |\psi\rangle = X|\psi\rangle$ when $x=1, z=0$

$X^x Z^z |\psi\rangle = Z|\psi\rangle$ when $x=0, z=1$

$X^x Z^z |\psi\rangle = XZ|\psi\rangle$ when $x=1, z=1$

Suppose $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

w.p. $\frac{1}{4}$, $x=0, z=0$, $\rho_{00} = |\psi\rangle\langle\psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix}$

$= \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{bmatrix}$

w.p. $\frac{1}{4}$, $x=1, z=0$, $\rho_{10} = X \rho_{00} X^\dagger$

$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$= \begin{bmatrix} \beta\alpha^* & |\beta|^2 \\ |\alpha|^2 & \alpha\beta^* \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$= \begin{bmatrix} |\beta|^2 & \beta\alpha^* \\ \alpha\beta^* & |\alpha|^2 \end{bmatrix}$

w.p. $\frac{1}{4}$, $x=0$, $z=1$.

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ -\beta\alpha^* & -|\beta|^2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} |\alpha|^2 & -\alpha\beta^* \\ -\beta\alpha^* & |\beta|^2 \end{bmatrix}$$

w.p. $\frac{1}{4}$, $x=1$, $z=1$.

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} |\alpha|^2 & -\alpha\beta^* \\ -\beta\alpha^* & |\beta|^2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} |\beta|^2 & -\beta\alpha^* \\ -\alpha\beta^* & |\alpha|^2 \end{bmatrix}$$

$$\rho = \frac{1}{4}\rho_{00} + \frac{1}{4}\rho_{10} + \frac{1}{4}\rho_{01} + \frac{1}{4}\rho_{11}$$

$$= \frac{1}{4}\left(\begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{bmatrix} + \begin{bmatrix} |\beta|^2 & \beta\alpha^* \\ \alpha\beta^* & |\alpha|^2 \end{bmatrix} + \begin{bmatrix} |\alpha|^2 & -\alpha\beta^* \\ -\beta\alpha^* & |\beta|^2 \end{bmatrix} + \begin{bmatrix} |\beta|^2 & -\beta\alpha^* \\ -\alpha\beta^* & |\alpha|^2 \end{bmatrix} \right)$$

$$= \frac{1}{4}\begin{bmatrix} 2(\underbrace{|\alpha|^2+|\beta|^2}_{=1}) & 0 \\ 0 & 2(|\alpha|^2+|\beta|^2) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{\mathbb{I}}{2} .$$