Name and St.ID#:_____

CSE439, Fall 2025 Prelim II Nov. 20, 2025

Open book, open notes, closed neighbors, 75 minutes. The exam totals 100 pts., subdivided as shown. Do *all five problems* on these exam sheets—there is no "choice" option. *Show your work*—this may help for partial credit.

Use of a quantum circuit simulation app—whether online or downloaded—or matrix calculator is forbidden. You may use—and cite—theorems and facts from lectures and homeworks without further justification.

Notation: You may freely mix "standard linear algebra notation" and "Dirac *bra-ket* notation" for quantum states. For example, e_{10} means the same thing as $|10\rangle$ and is represented (in big-endian notation) by the unit column vector $[0,0,1,0]^T$. The vectors $|+\rangle = \frac{1}{\sqrt{2}}[1,1]^T$ and $|-\rangle = \frac{1}{\sqrt{2}}[1,-1]^T$ really don't have good "non-Dirac" names, however, and for matrix outer-products the *ket-bra* form typified by $|+\rangle\langle -|$ is standard. Quantum state vectors use big-endian notation by default; if you switch to little-endian you must say so. *The problems begin overleaf.*

(1) (25 pts. total) *True/False with justifications.*

Please write out the words `true` or `false` in full in the blanks below, **and** write justifications next to them. Justifications are **required** and worth 3 of the 5 points for each question.

(a) Given any n-variable Boolean formula ϕ with the property that exactly one assignment $s \in \{0,1\}^n$ makes $\phi(s) = \mathit{true}$, Grover's algorithm can find s with high probability in $n^{O(1)}$ time.

(b) Given any n-variable Boolean function f with the property that exactly one string $s \in \{0,1\}^n$ makes $f(x) = f(y) \iff x \oplus y = s$ hold for all $x, y \in \{0,1\}^n$, Simon's algorithm can find s with high probability in $n^{O(1)}$ time.

(c) If U is an $n \times n$ matrix and $U\left(\frac{x+y}{2}\right) = \frac{1}{2}\left(U(x) + U(y)\right)$ for all vectors $x, y \in \mathbb{C}^n$, then U is unitary.

(d) The difference of two Hermitian matrices is Hermitian.

(e) The tensor product of two Hermitian matrices is Hermitian.

(a) _____

(b) _____

(c) _____

(d) _____

(e) _____

(2) (15 + 9 = 24 pts.)

(a) Use the spectral method to compute a 2×2 matrix $\mathbf{U}$ such that $\mathbf{U}^4 = \mathbf{X}$, i.e., $\mathbf{U}$ is a *fourth* root of NOT. You may take it as given that $|+\rangle$ and $|-\rangle$ form an orthonormal eigenbasis for $\mathbf{X}$. Show all steps from then on. You may use ω to abbreviate $+\sqrt{i} = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$.

(b) Recall that the *square* root of NOT, which we called $\mathbf{V}$, satisfied $\mathbf{V} = \mathbf{HSH}$. Use a similar idea to compute $\mathbf{U}$ a different way. Did you get exactly the same answer as in part (a)?

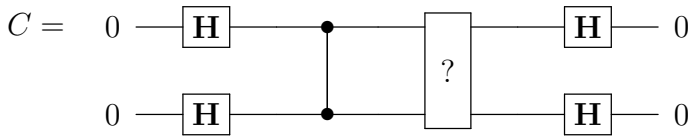
(3) (9+9 = 18 pts.) *Two short-answer questions*

(a) Show that if A and B are Hermitian matrices that do not commute (i.e., $AB \neq BA$), then AB *cannot be* Hermitian. For instance, $\mathbf{ZH} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$, which is not Hermitian.

(b) For $M = 77$, find a number $X < M$ that you would want to get as $a^{r/2} \pmod{M}$, when quantum runs of Shor's algorithm give you the true period r of the number a (which is relatively prime to M and less than M). For full credit, your number X must have $X^2 \equiv 1 \pmod{M}$, but without a calculator to hand, you may presume this is true when *both* $X - 1$ and $X + 1$ give a factor via gcd with M.

(4) (18 pts. total)

Consider the following two-qubit circuit with a "mystery gate." It happens to be a graph-state circuit otherwise, and we have shown it with $|00\rangle$ as input and testing for the same output:



(a) Suppose the mystery gate is absent—i.e., the identity. What is the amplitude $\langle 00| C |00\rangle$?

(b) Suppose the mystery gate is another **CZ**. What is $\langle 00| C |00\rangle$ now?

(c) Suppose the gate is $\mathbf{Z} \otimes \mathbf{I}$—i.e., we just add a loop at node 1. Then what is $\langle 00| C |00\rangle$?

(d) Suppose the gate is "$(-1)^{NAND}$" following conventions we've used before: it leaves $|11\rangle$ alone but multiplies the other three basis states by -1. What does that do to the amplitude $\langle 00| C |00\rangle$? Is it the same amplitude as in (b)? Is the probability of getting $|00\rangle$ as measurement outcome the same as in (b)? [Using "maze diagrams" is highly advised.]

(5) (15 pts.—end of exam)

Let G be an undirected graph on some number n of vertices (self-loops allowed), and let C_G be the corresponding graph-state circuit. Prove that $\langle +^n | \, C_G \, | +^n \rangle$ cannot equal 0, regardless of what G is. What value do you actually get?

For **6 pts. exam extra credit**, explain why the following argument doesn't contradict the above: "Take G to be a graph for which $\langle 0^n | \, C_G \, | 0^n \rangle = 0$, such as the triangle graph with $n = 3$. Recall from problem (1) of Assignment 4 that it follows that $\langle x | \, C_G \, | x \rangle = 0$ for all $x \in \{0,1\}^n$. By the principle of linearity, since $|+^n\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$ (where as usual $N = 2^n$), we have:

$$\langle +^n | \, C_G \, | +^n \rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} \langle x | \, C_G \, | x \rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} 0,$$

using the fact from Assignment 4. Thus $\langle +^n | \, C_G \, | +^n \rangle = 0$." There is a flaw here, indeed a lie. What is it?