CSE439, Fall 2025 **Final Exam** **Dec. 16, 2025**

Open book, open notes, closed neighbors, 170 minutes after a 10-minute read-through period. The exam has six problems totaling 234 points, subdivided as shown, *plus* an 6 pt. extra-credit question at the end. *Show all work in the exam books provided*—this may help for partial credit. Use of a quantum circuit simulation app—whether online or downloaded—or matrix calculator is forbidden. Some parts have helps on steps where such an app might be used. 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 $[0, 0, 1, 0]^T$. For matrix outer-products the *ket-bra* form typified by $|+\rangle\langle -|$ **is** standard. The notation $\langle u \mid v\rangle$ is the same as $\langle u, v\rangle$ for inner product. Quantum state vectors use big-endian notation by default; if you switch to little-endian you must say so. The conjugate transpose of a matrix U is denoted by U^*.

(1) ($5 \times 6 = 30$ pts. total) *Multiple choice with justifications*—Each question has a unique *best answer*, and a justification for it is **required** to earn the full 6 points. The justification need not be a full proof—one pertinent sentence will do. Reasons to reject other options are not necessary, but could even gain full credit by themselves if they convincingly reinterpret that option to make it reasonable.

1. Shor's Algorithm will generally continue to work as intended under which kind of noise?
   (a) Randomly flipping bits of the n-bit representation of the number M being factored.
   (b) Randomly adding $+1$ or -1 to values of $f_a(x) = a^x \pmod M$.
   (c) Rounding phases of the Quantum Fourier Transform to the nearest $\frac{1}{16}$ of a circle.
   (d) Noise that implicitly measures deeply-entangled n-qubit states, such as $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f_a(x)\rangle$.

2. The CHSH Game:
   (a) Is a simple stand-alone computational problem like factoring, but, unlike Shor's algorithm, gives proven quantum advantage.
   (b) Proves that quantum states do not "collapse" when measured.
   (c) Requires the two parties (called "Alice" and "Bob" in text and lecture) to share entangled qubits before they start playing the game.
   (d) Requires the two parties to communicate at faster than light speed.

3. If A is a Hermitian matrix, then:
   (a) At least one eigenvalue of A is zero.
   (b) The matrix A^{-1} is also Hermitian.

(c) The matrix iA is also Hermitian.

(d) The matrix A^2 is also Hermitian.

4. If A is any matrix (over the complex numbers) then:

   (a) A^*A and AA^* are always defined and always square matrices.

   (b) The tensor product $A \otimes A$ is defined only when A is square.

   (c) The SVD of A is defined only when A is square.

   (d) The product of A with a vector of all 1s is zero only if A is the all-zero matrix.

5. The quantum **T** gate:

   (a) Can be simulated by a concatenation of Hadamard, $\mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$, and the Pauli gates.

   (b) Preserves the quantum states $|0\rangle$ and $|1\rangle$ and hence rotates around the vertical axis of the Bloch sphere.

   (c) In conjunction with the Hadamard and CNOT gates, allows every other one- or two-qubit gate to be represented exactly.

   (d) Is Hermitian as well as unitary.

(2) (9+3+9+12 = 33 pts. total)

Note that the Toffoli gate computes the reversible form of the binary AND function: $\mathbf{Tof}(x_1, x_2, z) = (x_1, x_2, z \oplus x_1 \wedge x_2)$. If we put Hadamard gates on lines 1 and 2 before it, then we get the functional superposition of AND, namely $\sum_{x_1 x_2 \in \{0,1\}^2} |x_1 x_2\rangle |x_1 \wedge x_2\rangle$. (The input is presumed to be $|000\rangle$.)

(a) Design a quantum circuit C on three qubits to compute the functional superposition of the binary XOR function. (This does not need the Toffoli gate or any other 3-qubit gates.)

(b) Purely for cosmetic reasons, add a fourth qubit line so that you get (the functional superposition of) XOR repeated twice: $f(x_1 x_2) = (x_1 \oplus x_2)(x_1 \oplus x_2)$, so that f is a function from $\{0,1\}^2$ to $\{0,1\}^2$—i.e., on the binary strings of length 2.

(c) Show that the function f in part (b) is 2-to-1 with a "hidden string" s in the sense of Simon's Algorithm. What is s?

(d) Now create C' by appending two more Hadamard gates on lines 1 and 2. It does not matter whether you do this to your three-qubit circuit C in (a) or the four-qubit circuit in (b), because we will ignore results from the third and/or fourth qubit anyway. Show that in any measurement outcome, qubits 1 and 2 give either 00 or give 11. (Again, all-0 input is presumed. There is a high-level way to prove this without needing any matrix-vector calculations. If you do the latter, you may-or-may-not find it easier to convert C into an equivalent graph-state circuit with Hadamard gates on line 3 as well.)

(3) (9 + 9 + 12 + 18 = 48 pts. total)

Consider the following 4-vertex graph $G_0 = (V_0, E_0)$ with $V_0 = \{1, 2, 3, 4\}$ and $E = \{(1, 4), (2, 4), (3, 4), (4, 4)\}$. That is, node 4 is connected to every node, including a self-loop, but there are no other edges.

(a) Draw the corresponding graph-state circuit C_0 of four qubits, numbered as above. This time we *include* the second bank of Hadamard gates and tell you that on input $|0000\rangle$, the output state is $\Phi_0 = \frac{1}{2}(|0000\rangle + |0001\rangle + |1110\rangle + |1111\rangle)$.

(b) Demonstrate formally that nodes 1, 2, and 3 are collectively entangled with node 4.

(c) Now let ρ be the state that results from tracing out nodes 3 and 4 and answer: is it a pure state, and is it entangled? (It is possible to answer this without writing out a whole 16×16 density matrix.)

(d) Now let G be an *arbitrary* graph of n nodes that has at least two nodes t and u that are **not** connected by an edge. Make a new graph G' of $n + 2$ nodes by sticking in a copy of G_0 where node 1 is t, node 2 is u, and nodes 3 and 4 are new (you can call them v and w if you wish). Let C' be the corresponding graph-state circuit. Prove that

$$\langle 0^{n+2} \mid C' \mid 0^{n+2} \rangle = \frac{1}{2} \langle 0^n \mid C \mid 0^n \rangle,$$

where C is the graph-state circuit of G. Thus if G is net-zero, then so is G'. (For an interesting base case to help you start, let G have just two vertices t, u and no edges. Then G is *not* net-zero, indeed $\langle 00 \mid C \mid 00 \rangle = 1$. And G' is just the graph G_0 above—and $\langle 0000 \mid C' \mid 0000 \rangle = \frac{1}{2}$ just as shown in the state Φ_0 above, so it checks out. On the other hand, if you give the otherwise-empty G a self-loop at node t and/or node u, then it is net-zero, and so is the resulting G' which adds one or two extra self-loops to G_0.)

(4) (9+12+12 = 33 pts.) *Short-answer questions.* A single pithy sentence may suffice; general expectation is a paragraph of 2–4 sentences.

(a) Let $\mathcal{M}(\Phi)$ stand for the operation of measuring a quantum state Φ. If Φ is a linear combination $a\Phi_0 + b\Phi_1$ of two other legal states, does it follow that $\mathcal{M}(\Phi) = a\mathcal{M}(\Phi_0) + b\mathcal{M}(\Phi_1)$? Why or why not?

(b) The Sieve of Eratosthenes is a classical brute-force algorithm that finds a proper factor p of a composite number M in $O(\sqrt{M})$ time. Can Grover's algorithm at least match that time on a quantum computer, or even improve it?

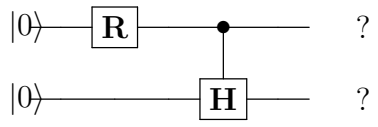
(c) Why isn't Simon's algorithm considered to separate quantum polynomial time (BQP) from classical deterministic polynomial time (P)? This is even though Daniel Simon's paper proved that no deterministic polynomial time algorithm can solve the problem of finding hidden strings of 2-to-1 functions f (when they exist) by querying values $f(x)$.

(5) (6 + 9 + 9 + 6 + 18 = 48 pts.)

(a) The *controlled Hadamard gate* **CH** is a two-qubit gate with a control on line 1 and Hadamard gate on line 2. Write out its 4×4 unitary matrix.

(b) Complete the unitary matrix $\mathbf{R} = \begin{bmatrix} \frac{1}{\sqrt{3}} & ? \\ ? & ? \end{bmatrix}$. (Make the upper-right corner negative.)

(c) Show that the following circuit produces the quantum state $\Phi = \frac{1}{\sqrt{3}}(|00\rangle + |10\rangle + |11\rangle)$. (Here, no shortcut to avoid multiplying 4×4 matrices is intended.)



(d) Reshape Φ into a 2×2 matrix F and say why it shows that Φ is entangled.

(e) Compute expressions for the singular values σ_1 and σ_2 of F. *Don't* try to evaluate the expressions numerically or compute the associated U or V matrices. But even without a calculator, you should be able to compare σ_1 and σ_2 (or their squares) well enough to say whether the SVD truncation technique would give a "good" or "coarse" approximation to Φ by a separable state.

(6) (9 + 9 + 18 + 6 = 42 pts.)

(a) Recall the three-qubit **CCZ** gate and note that it can be called "$(-1)^{AND(x,y,z)}$" since it flips the phase of a basis state $|xyz\rangle$ if and only if $x = y = z = 1$. Using **CCZ** and single-qubit gates only, design a sequence of quantum gates—which you could call as a 3-qubit "macro gate" **OOZ**—that computes "$(-1)^{NOR(x,y,z)}$." This means that "**OOZ**" flips the phase only of the $|000\rangle$ component of a state.

(b) Now take the three-node triangle graph and its graph state circuit, this time *skipping* the second Hadamard transform (all this so far as on problem 2 of Assignment 7), and then add the **CCZ** and **OOZ** gates (one of each—order does not matter). Calculate the resulting three-qubit pure state Φ.

(c) Calculate whether Φ is (i) a tensor product of three single-qubit pure states, (ii) a tensor product of a single-qubit pure state and an entangled two-qubit pure state, or (iii) not separable at all.

(d) Also answer: if you trace out qubit 3, are you left with a pure state of two qubits? What state do you get? Is it entangled?

Bonus: If A is Hermitian, then is e^{iA} always Hermitian? Is e^{iA} always invertible? Justifications are needed to collect **3+3=6** extra-credit points.

End of Exam