CSE439 Practice Final Exam Fall 2024

Open book, open notes, closed neighbors, 170 minutes after a 10-minute read-through period. The exam totals 267 pts., subdivided as shown. Do *all seven problems* on these exam sheets. em Always 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 $[0, 0, 1, 0]^T$. Non-unit vectors should only use the standard notation. 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.

[Your actual final exam will use exam booklets. Its formatting will be close to this but will differ somewhat.]

(1) (3 × 15 = 45 pts.) *Short-answer questions.* A single pithy sentence may suffice; general expectation is a paragraph of 2–4 sentences. (This is technically the same as **true/false with justifications** but with longer questions.)

(a) If A and B are unitary matrices, must $\frac{1}{\sqrt{2}}(A + B)$ be unitary? If you say yes, prove it; if you say no, give a concrete counterexample.

(b) Suppose you know in advance that a Grover search problem has exactly one solution $y \in \{0, 1\}^n$. The Grover oracle reflects about the "miss vector" $\mathbf{m}_{\{y\}}$, and the "hit vector" $\mathbf{h}_{\{y\}}$ is a simple linear combination of $\mathbf{m}_{\{y\}}$ and the all-1s vector $\mathbf{j}$ (which is easily computed via $\mathbf{H}^{\otimes n}|0^n\rangle$). Explain as best you can why Grover's algorithm cannot simply jump to $\mathbf{h}_{\{y\}}$ in one iteration step and then measure to give y with virtually 100% probability.

(c) Suppose $M = pq$ is a product of two odd primes and a is relatively prime to M with $1 < a < M$. Then $z = a^2 \pmod M$ is a quadratic residue modulo M. Find a different number $b < M$ such that $b^2 \bmod M = z$, show this, and say why $b \neq a$.

(2) (9+6+15 = 30 pts. total)

Make a quantum circuit of two qubits—both initialized to $|0\rangle$—with the following gates:

1. A Hadamard on line 1 only.
2. A CNOT gate with control on line 1 and target on line 2.
3. An **S** gate on line 1. (This is also called the *phase gate* and has matrix $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.)
4. Another CNOT gate with control on line 1 and target on line 2.

(a) Calculate the resulting two-qubit state ϕ.

(b) Is ϕ entangled? Prove your answer.

(c) Now replace the second CNOT gate by a **CZ** gate on the same two qubits. Calculate the final state ϕ' now and again say whether it is entangled.

(3) (12 + 6 + 9 + 9 + 6 = 42 pts. total)

Make a quantum circuit C on three qubits by placing the following gates:

1. Hadamard gates on all three lines.
2. A CZ gate between lines 1 and 2.
3. A CNOT gate with control on line 1 and target on line 3.
4. A CZ gate between lines 2 and 3.
5. Hadamard gates on all three lines again.

This differs from a graph-state circuit only in having the CNOT gate.

(a) Compute $\langle 0^n \mid C \mid 0^n \rangle$ *without* resorting to 8×8 matrix multiplications. Using a "maze diagram" is fine, but there are methods even shorter than that.

(b) Compute the state ϕ that was present before the final three Hadamard gates—that is, after the second **CZ** gate. (This might already be part of your answer to part (a).)

(c) Compute the density matrix $\rho = |\phi\rangle \langle\phi|$. (OK, this is tedious—but you get 9 pts. for it.)

(d) Trace out qubit 3 from ρ.

(e) Does the resulting 2-qubit density matrix ρ' represent a pure state? a completely mixed state? a mixed state but not completely mixed? Justify your answer.

(4) (36 pts. total)

Let A be the Hermitian PSD matrix $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$.

(a) Find its spectral decomposition $A = \lambda_1 |u_1\rangle \langle u_1| + \lambda_2 |u_2\rangle \langle u_2|$.

(b) Calculate $U = e^{i\pi A}$ by replacing λ_1 with $e^{i\pi\lambda_1}$ and ditto for λ_2.

(c) Say briefly why U is unitary. What quantum operation (if any) does it represent?

(5) (12 + 6 + 24 = 42 pts.)

Make a quantum circuit of two qubits—both initialized to $|0\rangle$—by placing the following gates:

1. A Hadamard gate on line 1 only.
2. Then a **T**-gate on line 1 only.
3. A CNOT gate with control on line 1 and target on line 2.
4. Another Hadamard gate on line 1.

(a) Calculate the final quantum state ϕ of two qubits.

(b) Show that ϕ is entangled.

(c) Use the SVD truncation technique to approximate ϕ by a separable state $\alpha \otimes \beta$.

(6) (36 pts. total)

Design a quantum circuit C of 3 qubits that on input $|000\rangle$ prepares the pure state

$$\frac{1}{2}\left(|001\rangle - |011\rangle - |100\rangle + |111\rangle\right).$$

(7) ($6 \times 6 = 36$ pts. total) *Multiple choice*—no justifications are required but may help for partial credit:

1. If a one-qubit quantum state $|\phi\rangle$ is measured in an orthonormal basis $B_1 = \{|u_1\rangle, |v_1\rangle\}$ versus another orthonormal basis $B_2 = \{|u_2\rangle, |v_2\rangle\}$, then:

   (a) The probability of outcome $|u_1\rangle$ using B_1 will be the same as that of outcome $|u_2\rangle$ using B_2.

   (b) The probability of outcome $|u_1\rangle$ using B_1 will either be the same as that of the outcome $|u_2\rangle$ using B_2 or the outcome $|v_2\rangle$ using B_2, because the basis could be listed either way.

   (c) One could have the probability of outcomes $|u_1\rangle$ versus $|v_1\rangle$ be 50-50 while the probability of outcomes $|u_2\rangle$ versus $|v_2\rangle$ could be 75% versus 25%.

   (d) It is possible for both the probability of getting $|u_2\rangle$ and the probability of getting $|v_2\rangle$ to be zero when the basis B_2 is used.

2. A three-qubit quantum circuit C with the property that for any single-qubit pure state $|\phi\rangle$, C on input $|\phi\rangle \otimes |0\rangle \otimes |0\rangle$ outputs $|0\rangle \otimes |\phi\rangle \otimes |\phi\rangle$ is:

(a) Built simply by placing Hadamard on line 1, then two CNOT gates with controls on line 1 and targets on lines 2 and 3, respectively, and finally another Hadamard gate on line 1.

(b) Buildable by modifying the circuit in the text for "teleporting" an arbitrary qubit $|\phi\rangle$.

(c) Impossible, as shown by the No-Cloning Theorem.

(d) Impossible, by Holevo's theorem that n qubits can yield only n bits of classical information.

3. A unitary 4×4 matrix:

   (a) Always has positive real eigenvalues.

   (b) May have 0 as an eigenvalue.

   (c) Has only eigenvalues of the form $e^{i\theta}$ for some angle θ, $0 \leq \theta < 2\pi$.

   (d) Has eigenvalues whose squares sum to 1.

4. A Hermitian 4×4 matrix:

   (a) Always has positive real eigenvalues.

   (b) May have 0 as an eigenvalue.

   (c) Has only eigenvalues of the form $e^{i\theta}$ for some angle θ, $0 \leq \theta < 2\pi$.

   (d) Has eigenvalues whose squares sum to 1.

5. The CHSH Game is significant because:

   (a) It proves that faster-than-light communication is possible.

   (b) No physical system that operates only locally—without using non-local quantum entanglement—can achieve success probability over 75% in the long run of repeated trials.

   (c) Experiments have achieved success probability over 80%—nearing the theoretical 85.3...%—by quantum means (winning a Nobel Prize, incidentally).

   (d) Two of the above statements are true but the other is not true.

6. Shor's Algorithm:

   (a) Has been used to factor integers of over 1,000 digits of the kind used in RSA encryption with consistent success.

   (b) Solves a problem in quantum polynomial time that classical computers have been proved not to be able to solve in deterministic polynomial time.

   (c) Challenges the assertion that natural processes can always be modeled precisely and efficiently in a computer language like C++.

   (d) Cannot be executed using quantum circuits that have only Hadamard, CNOT, and **T**-gates.

END OF EXAM