There are five pages including this cover page. You have 60 minutes. No notes, books, calculators, computers, etc. are allowed.

Some problems explicitly declare that no explanation is necessary. On all other problems, show your work, in as organized a manner as possible. Incorrect answers with solid work often earn partial credit. Correct answers without explanatory work rarely earn full credit. Perform as much algebraic simplification as you can.

You may cite without proof any result discussed in class, the assigned textbook sections, or the assigned homework.

Good luck. :)

A. Fill in the blanks. No explanation is necessary on Problem A.

A.A. Excluding measurements, any n-qbit gate can be viewed as a(n) ________ ________ matrix.

A.B. If U and V are n-qbit gates, then $U \otimes V$ is a(n) ________-qbit gate.

A.C. If U and V are n-qbit gates, then $U \cdot V$ is a(n) ________-qbit gate.

A.D. In the worst case, the Bernstein-Vazirani algorithm invokes the oracle f ________ time(s).

A.E. For any classical n-qbit state $|\alpha\rangle$, $H^{\otimes n} |\alpha\rangle = \sum_{\beta \in \{0,1\}^n}$ ________ $|\beta\rangle$.

A.F. The construction $|\alpha\rangle |\beta\rangle \mapsto$ ________________, for all $\alpha \in \{0,1\}^n$ and $\beta \in \{0,1\}^m$, turns any classical function $f : \{0,1\}^n \to \{0,1\}^m$ into its corresponding quantum gate.

B.A. Write out the matrix that represents the quantum version of the classical AND gate.

B.B. Mermin uses two special names for this gate, other than AND. What are they?

C. These are TRUE/FALSE/PUNT questions. No explanation is necessary on Problem C. Correct answers earn full credit, incorrect answers earn no credit, and PUNT earns half credit.

C.A. Any n-qbit state is a linear combination of tensor products of 1-qbit states.

C.B. $H^{\otimes 4}\left|++-+\right\rangle$ is a classical state.

C.C. After partial measurement of the last m qbits in an $(n+m)$-qbit system, the first n qbits are always unentangled from the last m qbits.

C.D. It is possible for partial measurement of the last 3 qbits of a 5-qbit system in state $\left|-++++\right\rangle$ to put the system into state $\left|10000\right\rangle$.

D. Let $\omega = 10011$. Draw a possible circuit diagram for the quantum gate f that is used in the Bernstein-Vazirani algorithm.

E. Simon's algorithm solves Simon's problem. What a coincidence.

E.A. Draw the circuit diagram for the crucial, quantum subroutine of Simon's algorithm.

E.B. Explain in plain English (not mathematical notation) how that subroutine is used to solve the problem. Perhaps your answer should mention how many times the subroutine runs.

F. This problem is about Grover's algorithm. Assume that $\left|f^{-1}(1)\right| = m \geq 1$ is known.

F.A. As m increases, does the problem get easier or harder? In other words, does the algorithm perform better or worse? (A strong answer addresses at least three issues.)

F.B. Give a practical application of Grover's algorithm with known $m \geq 1$. For that problem, how does Grover's running time compare to the best classical running time known?