Mid-term Exam

Name: _____

Spring 2019, CSCE 440/640 Quantum Algorithms — March 18, 2019

Texas A&M U — Prof. Fang Song

Instructions (please read carefully before start!)

- This take-home exam contains 9 pages (including this cover page) and 3 questions. Total of points is 85.
- You will have till **March 20, 2019, 11:59pm, AoE** (Anywhere on Earth) to finish the exam. You must work on your own, and no collaboration or help from any resources other than those made available in class (lecture notes, recommended texts, homework problems, etc.) is permitted.
- Email me your solutions in PDF before the deadline, either scanned or typeset in LaTeX. Name your PDF and email subject as: **Lastname_Firstname_s19_mt**. If you choose to hand-write and scan, *print out this exam sheet and write your solutions on it*. Do your best to fit your answers into the space provided, and attach extra papers only if necessary. If you typeset in LaTeX, *use the provided TeX file*. No other formats are accepted.
- Your work will be graded on correctness and clarity. Make sure your hand writing is legible.
- Don't forget to write your name on top (or update the "\studentname" command in the TeX file)!

Grade Table (for instructor use only)

Question	Points	Score
1	20	
2	40	
3	25	
Total:	85	

1. *Short answers*. Answer the following, and briefly justify your answer.

   (a) (0 points) (Sample problem) Is $\sqrt{i/3}|0\rangle + \sqrt{2/5}|1\rangle$ a valid quantum state?

   Solution: Answer: No.
   Justification: Because $|\sqrt{i/3}|^2 + |\sqrt{2/5}|^2 \neq 1$.

   (b) (5 points) Is $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ an entangled state?

   (c) (5 points) Quantum computers can solve NP-Complete problems in polynomial time. Is this statement True/False/Unknown?

   (d) (5 points) Recall in the quantum superdense coding protocol, Alice wants to send two classical bits to Bob by sending one qubit. Suppose a third party (Eve) intercepts Alice's qubit on the way. Can Eve infer anything about which of the four possible bit strings 00, 01, 10, 11 Alice was trying to send?

   (e) (5 points) What is the Quantum Fourier Transform F_{2^4} on a four-qubit state $\frac{1}{4}|0000\rangle + \frac{i}{4}|0010\rangle + \sqrt{\frac{5}{8}}|1111\rangle$?

2. (Quantum circuits)

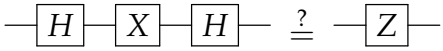
(a) (10 points) Suppose you have an unlimited supply of qubits in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and qubits in the state $|0\rangle$. Give quantum circuits and specify the inputs for producing the following quantum states:

i) $\alpha^2|00\rangle - \alpha\beta|01\rangle + \alpha\beta|10\rangle - \beta^2|11\rangle$.

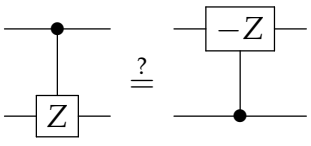
ii) $\alpha|00\rangle - \beta|11\rangle$.

(b) (20 points) For each pair of the circuits below, prove or disprove that they are equivalent.

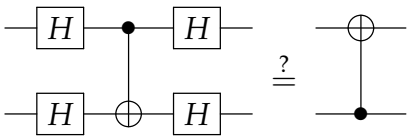
i)



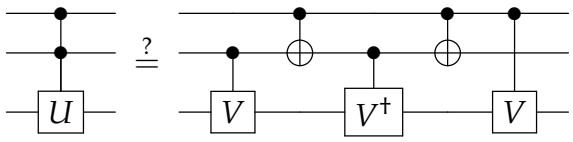
ii)



iii)



iv) Let U, V be unitary, and $V^2 = U$. The left-hand-side is U controlled by two qubits $|a\rangle|b\rangle$ such that U is applied to the third qubit iff. $a = b = 1$.



(c) (5 points) Construct a CNOT gate from one controlled-Z gate and two Hadamard gates.

(d) (5 points) (Phase estimation: alternative) Let U be an n-qubit unitary operator and $|\psi\rangle$ be an eigenvector with $U|\psi\rangle = e^{i\theta}|\psi\rangle$. Analyze the circuit below and derive the probability that the measurement outcome is 0.

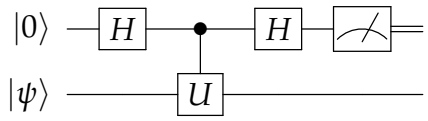


Figure 1: Alternative phase estimation algorithm

(e) (15 Bonus points) Continue from part (d).

i) How many times do we need to repeat the circuit in Figure d to get an estimate $\tilde{\theta}$ so that $|\theta - \tilde{\theta}| \leq \varepsilon$ with probability at least $1 - \delta$?

ii) Suppose you can replace U by U^k for an arbitrary integer k of your choice (still controlled by one qubit). Show how to approximate θ.

3. (Quantum algorithms and permutations) A bijection $P : \{0,1\}^m \to \{0,1\}^m$ is called a permutation on $\{0,1\}^m$.

   (a) (5 points) How many permutations are there in total on $\{0,1\}^m$?

   (b) (6 points) Let S be the set of all permutations on $\{0,1\}^m$. Consider a subset $\{P_k\} \subseteq S$ which are indexed by n-bit keys $k \in \{0,1\}^n$ for some $n \leq m$. We are now given $(x_1, \ldots, x_t)$ and $(y_1, \ldots, y_t)$ with the promise that there is a *unique* $k^* \in \{0,1\}^n$ such that $P_k(x_i) = y_i$ for all $i = 1, \ldots, t$. The goal is to identify this key k^*. Let us consider classical algorithms first. Suppose we have access to an oracle $O : (k, x) \mapsto P_k(x)$. How many queries are sufficient to determine k^* in the worst case? How many are necessary? Justify your answer.

   (c) (14 points) Continue from above. Suppose O can be queried in quantum superposition, i.e., it is given as a black-box quantum circuit implementing the unitary

$$U : |k\rangle|x\rangle|y\rangle \mapsto |k\rangle|x\rangle|y \oplus P_k(x)\rangle, \forall k \in \{0,1\}^n, x, y \in \{0,1\}^m .$$

   i) Show that one can implement another quantum oracle

$$U' : |k\rangle|b\rangle \mapsto |k\rangle|b \oplus f(k)\rangle ,$$

   where $f : \{0,1\}^n \to \{0,1\}$ is such that $f(k) = 1$ iff. $P_k(x_i) = y_i$ for all $i = 1, \ldots, t$. How many calls to U are needed to answer one query to U'?

(Problem 3.c continued)

ii) Give a quantum algorithm for finding k^*. Describe its cost in terms of # of queries to U and the circuit size.

(d) (15 Bonus points) Let $k_1, k_2 \in \{0,1\}^n$ be two secret strings and $\pi : \{0,1\}^n \to \{0,1\}^n$ be a permutation. Define another permutation[1] $P_{k_1,k_2} : \{0,1\}^n \to \{0,1\}^n$ as

$$P_{k_1,k_2} : x \mapsto \pi(x \oplus k_1) \oplus k_2 \,.$$

i) Define a function f from π and P_{k_1,k_2} such that for all x, $f(x \oplus k_1) = x$.

[1] This is the Even-Mansour block cipher.

ii) Suppose π is sampled uniformly at random among all permutations on $\{0,1\}^n$. Given quantum oracles for π and P_{k_1,k_2}, describe a quantum algorithm that recovers k_1, k_2 efficiently.

Scrap paper – no exam questions here.