CMSC/PHYS 457, Introduction to Quantum Computing
Spring 2025, University of Maryland

Due: April 1st, 2025
Date: March 10th, 2025

Assignment 2

Please submit it electronically to ELMS. This assignment is 8% in your total points. For the simplicity of the grading, the total points for the assignment are 80. Note that we will reward the use of Latex for typesetting with bonus points (an extra 5% of your points).

Problem 1. *The Hadamard gate and qubit rotations*

1. *(3 points)* Suppose that $(n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector and $\theta \in \mathbb{R}$. Show that
$$e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)} = \cos(\tfrac{\theta}{2})\, I - i\sin(\tfrac{\theta}{2})\,(n_x X + n_y Y + n_z Z).$$
2. *(3 points)* Find a unit vector $(n_x, n_y, n_z) \in \mathbb{R}^3$ and numbers $\phi, \theta \in \mathbb{R}$ so that
$$H = e^{i\phi} e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)},$$
where H denotes the Hadamard gate. What does this mean in terms of the Bloch sphere?
3. *(3 points)* Write the Hadamard gate as a product of rotations about the x and y axes. In particular, find $\alpha, \beta, \gamma, \phi \in \mathbb{R}$ such that $H = e^{i\phi} R_y(\gamma) R_x(\beta) R_y(\alpha)$.

Problem 2. *Universality of gate sets.* Prove that each of the following gate sets either is or is not universal. You may use the fact that the set $\{\textsc{cnot}, H, T\}$ is universal.

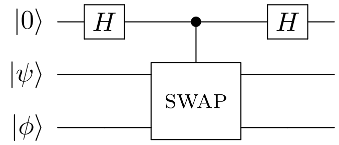
1. *(3 points)* $\{H, T\}$
2. *(3 points)* $\{\textsc{cnot}, T\}$
3. *(3 points)* $\{\textsc{cnot}, H\}$
4. *(Bonus: 5 points)* $\{\textsc{cnot}, H, T^2\}$

Problem 3. *Non-cloning theorem.* Please provide your answer and a brief explanation.

- *(5 points)* (Clone a random bit?) Given one sample of an unknown biased random coin (say, 0 with probability p and 1 with probability $1 - p$ and p unknown), is there a procedure to create two copies of such biased random coin? Namely, this procedure needs to generate two independent random coins with the same p.
- *(5 points)* (Clone one certain basis?) Is there a procedure to clone qubits restricted to $\{|+\rangle, |-\rangle\}$?
- *(Bonus: 5 points)* (Clone with many samples?) If you are given 1000 samples of an unknown biased random coin, is it possible to create 1,000,000 independent copies of the random coin? Here we allow the generated copies can be a little different from the original copy. Note that the precise number 1000 (or 1,000, 000) does not change the answer.

Problem 4. *Swap test.*

1. *(3 points)* Let $|\psi\rangle$ and $|\phi\rangle$ be arbitrary single-qubit states (not necessarily computational basis states), and let SWAP denote the 2-qubit gate that swaps its input qubits (i.e., $\text{SWAP}\,|x\rangle\,|y\rangle = |y\rangle\,|x\rangle$ for any $x, y \in \{0,1\}$). Compute the output of the following quantum circuit:



2. *(3 points)* Suppose the top qubit in the above circuit is measured in the computational basis. What is the probability that the measurement result is 0?

3. *(3 points)* If the result of measuring the top qubit in the computational basis is 0, what is the (normalized) post-measurement state of the remaining two qubits?

4. *(2 points)* How do the results of the previous parts change if $|\psi\rangle$ and $|\phi\rangle$ are n-qubit states, and SWAP denotes the $2n$-qubit gate that swaps the first n qubits with the last n qubits?

Problem 5. *Implementing the square root of a unitary.*

1. *(3 points)* Let U be a unitary operation with eigenvalues ± 1. Let P_0 be the projection onto the $+1$ eigenspace of U and let P_1 be the projection onto the -1 eigenspace of U. Let $V = P_0 + iP_1$. Show that $V^2 = U$.

2. *(3 points)* Give a circuit of 1- and 2-qubit gates and controlled-U gates with the following behavior (where the first register is a single qubit):

$$|0\rangle|\psi\rangle \mapsto \begin{cases} |0\rangle|\psi\rangle & \text{if } U|\psi\rangle = |\psi\rangle \\ |1\rangle|\psi\rangle & \text{if } U|\psi\rangle = -|\psi\rangle. \end{cases}$$

3. *(3 points)* Give a circuit of 1- and 2-qubit gates and controlled-U gates that implements V. Your circuit may use ancilla qubits that begin and end in the $|0\rangle$ state.

Problem 6. *The Bernstein-Vazirani problem.*

1. *(3 points)* Suppose $f : \{0,1\}^n \to \{0,1\}$ is a function of the form

$$f(\underline{x}) = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \bmod 2$$

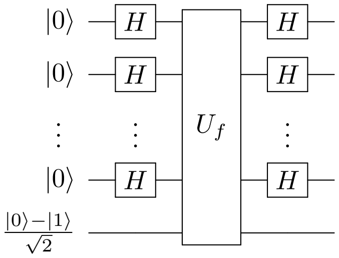
for some unknown $\underline{s} \in \{0,1\}^n$. Given a black box for f, how many classical queries are required to learn s with certainty?

2. *(3 points)* Prove that for any n-bit string $\underline{u} \in \{0,1\}^n$,

$$\sum_{\underline{v} \in \{0,1\}^n} (-1)^{\underline{u} \cdot \underline{v}} = \begin{cases} 2^n & \text{if } \underline{u} = \underline{0} \\ 0 & \text{otherwise} \end{cases}$$

where $\underline{0}$ denotes the n-bit string $00\ldots0$.

3. *(3 points)* Let U_f denote a quantum black box for f, acting as $U_f|\underline{x}\rangle|y\rangle = |\underline{x}\rangle|y \oplus f(\underline{x})\rangle$ for any $\underline{x} \in \{0,1\}^n$ and $y \in \{0,1\}$. Show that the output of the following circuit is the state $|\underline{s}\rangle(|0\rangle - |1\rangle)/\sqrt{2}$.



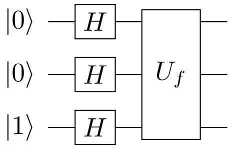
4. *(1 points)* What can you conclude about the quantum query complexity of learning s?

Problem 7. *One-out-of-four search.* Let $f\colon \{0,1\}^2 \to \{0,1\}$ be a black-box function taking the value 1 on exactly one input. The goal of the one-out-of-four search problem is to find the unique $(x_1, x_2) \in \{0,1\}^2$ such that $f(x_1, x_2) = 1$.

1. *(2 points)* Write the truth tables of the four possible functions f.
2. *(2 points)* How many classical queries are needed to solve one-out-of-four search?
3. *(5 points)* Suppose f is given as a quantum black box U_f acting as

$$|x_1, x_2, y\rangle \overset{U_f}{\mapsto} |x_1, x_2, y \oplus f(x_1, x_2)\rangle.$$

Determine the output of the following quantum circuit for each of the possible black-box functions f:



4. *(3 points)* Show that the four possible outputs obtained in the previous part are pairwise orthogonal. What can you conclude about the quantum query complexity of one-out-of-four search?

Problem 8. *Searching for a quantum state.*

Suppose you are given a black box U_ϕ that identifies an unknown quantum state $|\phi\rangle$ (which may not be a computational basis state). Specifically, $U_\phi|\phi\rangle = -|\phi\rangle$, and $U_\phi|\xi\rangle = |\xi\rangle$ for any state $|\xi\rangle$ satisfying $\langle\phi|\xi\rangle = 0$.

Consider an algorithm for preparing $|\phi\rangle$ that starts from some fixed state $|\psi\rangle$ and repeatedly applies the unitary transformation VU_ϕ, where $V = 2|\psi\rangle\langle\psi| - I$ is a reflection about $|\psi\rangle$.

Let $|\phi^\perp\rangle = \frac{e^{-i\lambda}|\psi\rangle - \sin(\theta)|\phi\rangle}{\cos(\theta)}$ denote a state orthogonal to $|\phi\rangle$ in $\mathrm{span}\{|\phi\rangle, |\psi\rangle\}$, where $\langle\phi|\psi\rangle = e^{i\lambda}\sin(\theta)$ for some $\lambda, \theta \in \mathbb{R}$.

1. *(2 points)* Write the initial state $|\psi\rangle$ in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.
2. *(2 points)* Write U_ϕ and V as matrices in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.
3. *(2 points)* Let k be a positive integer. Compute $(VU_\phi)^k$.
4. *(2 points)* Compute $\langle\phi|(VU_\phi)^k|\psi\rangle$.
5. *(2 points)* Suppose that $|\langle\phi|\psi\rangle|$ is small. Approximately what value of k should you choose in order for the algorithm to prepare a state close to $|\phi\rangle$, up to a global phase? Express your answer in terms of $|\langle\phi|\psi\rangle|$.