CMPT 476/981: Introduction to Quantum Algorithms
Assignment 2

Due **March 14th, 2024 at 11:59pm on coursys**
Complete individually and submit in PDF format.

Question 1 [4 points]: Gate approximation

Recall that the *approximation error* $E(U, V)$ of two unitaries U, V is defined as

$$E(U, V) = ||U - V|| = \max_{|\psi\rangle} ||(U - V)|\psi\rangle||$$

where the max above is over **pure states** $|\psi\rangle$ — that is, unit vectors.

1. Prove that approximation error is subadditive — that is, show that for any gates U_1, U_2, V_1, V_2,

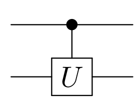
   $$E(U_2U_1, V_2V_1) \leq E(U_2, V_2) + E(U_1, V_1)$$

   You may use without proof two facts: the triangle inequality $||A + B|| \leq ||A|| + ||B||$ and $||UA|| = ||A|| = ||AU||$ for any unitary U and complex valued matrix A.

2. Suppose you have a circuit $U_1 \cdots U_k$ consisting of k gates and you wish to approximate over some particular gate set to an error of ϵ. What approximation factor should you choose for each gate?

Question 1 [2 points]: Controlled gates

Recall that a (quantum) controlled unitary is drawn as

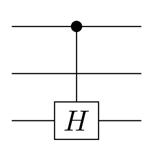


where the dot represents the control, and U is applied only when the control bit is in the state $|1\rangle$.

1. Verify that the following gives a controlled U gate for any unitary U:

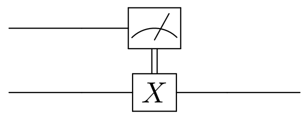
   $$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

2. Use the above expression to write the following circuit as a matrix



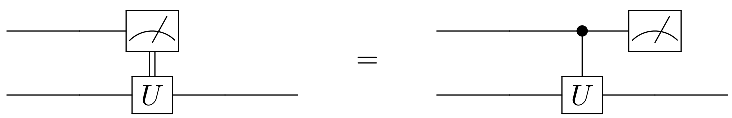
Question 2 [2 points]: Deferred measurement

A *classically controlled gate* U^x, $x \in \{0,1\}$ is a gate U which is applied if and only if the value of a *classical* (i.e. not in superposition) bit is 1. We've seen examples of classically controlled gates in class, with the superdense coding and teleportation protocols. In the case where x is a measurement outcome, we often draw the gate classically controlled on the x as



Here the double line denotes a *classical* bit, which is controlling whether or not to apply the X gate.

Show that every gate controlled on a measurement outcome is equivalent to a quantum controlled gate followed by a measurement. In circuit diagrams,



Question 3 [3 points]: Reversible circuits

Devise a reversible circuit composed of X, $CNOT$, and Toffoli gates computing the following function:

$$f(x_1, x_2, x_3, x_4, x_5) = (x_1 \oplus (x_2 \wedge x_3) \oplus x_4) \wedge (x_4 \oplus x_5 \wedge (\neg x_1 \wedge x_2)))$$

Your circuit should uncompute any temporary/intermediate values it uses.

Question 4 [3 points]: No garbage on Sundays

Suppose you have an oracle $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ for some classical function $f : \{0,1\} \to \{0,1\}$.

1. Give an explicit function f for which $U_f(\frac{1}{\sqrt{2}} \sum_{x\in\{0,1\}} |x\rangle|0\rangle)$ is an entangled state.

2. Let f be the function you showed was entangling in the last question. Show that measurement of the second qubit after applying U changes the state of the first qubit.

3. Suppose $f(x)$ is some intermediate value which we only needed temporarily in a larger computation. Why shouldn't we simply reset $|f(x)\rangle$ to $|0\rangle$ or $|1\rangle$ **by measuring it** in order to re-use it later?

Question 5 [5 points]: Bernstein-Vazirani

Recall that the Bernstein-Vazirani algorithm computes the **shift string** $s \in \mathbb{Z}_2^n$ hidden in some function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ where

$$f(x) = s \cdot x = s_1 x_1 \oplus s_2 x_2 \oplus \cdots \oplus s_n x_n$$

using an oracle $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ (or its phase version, $U_{\tilde{f}} : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$)

Let $n = 6$ and $s = 010111$.

1. Give an implementation of the oracle U_f using $CNOT$ gates.

2. Give an implementation of the oracle $U_{\tilde{f}}$. You may use any of the following: the oracle U_f, H, Z gates or ancillas initialized in $|0\rangle$ or $|1\rangle$.

3. Could the value of s be computed in polynomial time on a classical computer from your implementation of either U_f or $U_{\tilde{f}}$? Do you think query complexity is a good characterization of the problem in this case? What if instead U_f was any polynomial-sized oracle for f over the gate set consisting of X, $CNOT$, and Toffoli gates, with no other gaurantees about its structure?

Question 6 [6 points]: Simon's algorithm

Perform Simon's algorithm on the 3-bit function $f : \{0,1\}^3 \to \{0,1\}^3$ defined as

$$f(a,b,c) = (b(\neg a) + b(\neg c), b(a \oplus c), ac).$$

Specifically, do the following steps:

1. Write down the uniform superposition over values $f(x)$,

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^3} |x\rangle|f(x)\rangle.$$

2. Simulate measuring the output register $|f(x)\rangle$ by choosing some value of $c = f(x)$ that appears **with non-zero amplitude** in the above.

3. Apply $H^{\otimes 3}$ to the $|x\rangle$ register to get find the state

$$\frac{1}{\sqrt{|S^{\perp}|}} \sum_{z \in S^{\perp}} (-1)^{x \cdot z} |z\rangle|f(x)\rangle$$

4. Take samples of $|z\rangle$ from the above until you have $n - 1 = 2$ linearly independent vectors from $S^{\perp}$.

5. Solve the linear system $As = 0$ for s, where A is the matrix with rows given by the linearly independent vectors you previously sampled. This is your hidden string.