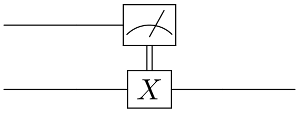
CMPT 476/776: Introduction to Quantum Algorithms
Assignment 3

Due **March 12th, 2026 at 11:59pm on crowdmark**
Complete individually and submit in PDF format.

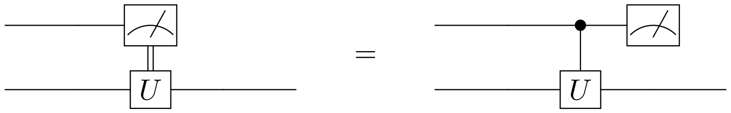
Question 1 [2 points]: Deferred measurement

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,

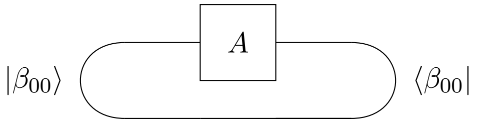


Question 2 [2 points]: Graphical trace

Let $|\beta_{00}\rangle = |00\rangle + |11\rangle$ be the (unnormalized) Bell state. Show that for any 2×2 matrix A,

$$\mathrm{Tr}(A) = \langle \beta_{00}|(A \otimes I)|\beta_{00}\rangle$$

In diagrammatic form we can draw this as



This equality extends to the partial trace as, e.g., $\mathrm{Tr}_B(\rho) = (I_2 \otimes \langle\beta_{00}|)(\rho \otimes I_2)(I_2 \otimes |\beta_{00}\rangle)$, and is particularly useful as it makes the trace *compositional*, in the sense that it can be defined entirely as the composition of linear operators. Compositional calculations like this are often easier to manipulate and *optimize* in a compiler or simulator. In *categorical quantum mechanics* one draws diagrams like these for most operations, e.g. teleportation.

Question 3 [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 $f : \{0,1\} \rightarrow \{0,1\}$.

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 4 [4 points]: Deutsch's interference

In class we saw that the Hadamard gate can be written as the mapping $|x\rangle \mapsto \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle$.

1. Show that HH maps $|x\rangle$ to $\frac{1}{2}\sum_{x,y,z}(-1)^{xy+yz}|z\rangle$
2. Let $c \in \{0,1\}$. Verify that $\frac{1}{2}\sum_{x,y}(-1)^{cx+xy}|y\rangle = |c\rangle$. In other words, the paths leading to y through the "intermediate state" x constructively interfere if and only if $y = c$.
3. Use this characterization of the Hadamard and the property from part 2 to give an alternate explanation of Deutsch's algorithm by explicitly showing that $HU_{\tilde{f}}H|0\rangle = |f(0)\oplus f(1)\rangle$ up to global phase, where $U_{\tilde{f}} : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$.

   Hint: Use the fact that $f(x) = (1\oplus x)f(0) \oplus xf(1) = (1+x)f(0) + xf(1) \mod 2$

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 $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ where

$$f(x) = s\cdot x = s_1x_1 \oplus s_2x_2 \oplus \cdots \oplus s_nx_n$$

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

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

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 $s \neq 0$, where A is the matrix with rows given by the linearly independent vectors you previously sampled. This is your hidden string.