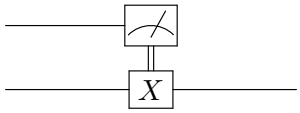
CMPT 476/776: Introduction to Quantum Algorithms
Assignment 3

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,

Solution. Let U be an operator on n qubits, and write the state of the $n+1$ qubits initially as $a|0\rangle|\psi_0\rangle + b|1\rangle|\psi_1\rangle$ where $|\psi_0\rangle$ and $|\psi_1\rangle$ are n-qubit unit vectors.

For the circuit on the left, the measurement produces the state $|0\rangle|\psi_0\rangle$ or $|1\rangle|\psi_1\rangle$ with probability $|a|^2$ and $|b|^2$, respectively. We only apply U in the case where the measurement result was 1, so the final ensemble of states is

$$\{(|0\rangle|\psi_0\rangle, |a|^2), (|1\rangle(U|\psi_1\rangle), |b|^2)\}$$

For the circuit on the right, we first apply the controlled-U gate to get the state

$$a|0\rangle|\psi_0\rangle + b|1\rangle(U|\psi_1\rangle).$$

Measurement then produces the ensemble

$$\{(|0\rangle|\psi_0\rangle, |a|^2), (|1\rangle(U|\psi_1\rangle), |b|^2)\}$$

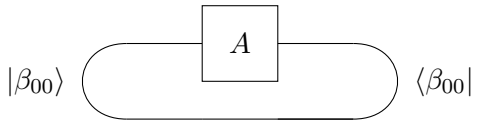
which is exactly the same ensemble of states as above. As a result, the final state on both sides has the same density matrix, and so they implement the same transformation.

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.

Solution. By direct calculation:

$$\begin{aligned}
\langle\beta_{00}|(A \otimes I)|\beta_{00}\rangle &= \begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix} \begin{bmatrix} A_{0,0} & 0 & A_{1,0} & 0 \\ 0 & A_{0,0} & 0 & A_{1,0} \\ A_{0,1} & 0 & A_{1,1} & 0 \\ 0 & A_{0,1} & 0 & A_{1,1} \end{bmatrix} \begin{bmatrix}1\\0\\0\\1\end{bmatrix} \\
&= \begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix} \begin{bmatrix} A_{0,0} \\ A_{1,0} \\ A_{0,1} \\ A_{1,1} \end{bmatrix} \\
&= A_{0,0} + A_{1,1} \\
&= \mathrm{Tr}(A)
\end{aligned}$$

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 $f : \{0,1\} \to \{0,1\}$.

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?

Solution.

1. Let $f(x) = x$. Then

$$U_f(\frac{1}{\sqrt{2}}\sum_{x\in\{0,1\}}|x\rangle|0\rangle) = \frac{1}{\sqrt{2}}\sum_{x\in\{0,1\}}|x\rangle|f(x)\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   which is a Bell state $|\beta_{00}\rangle$ and hence entangled.

2. Partial measurement of the second qubit in the computational basis for the state above produces the final state $|00\rangle$ or $|11\rangle$ with probability $\frac{1}{2}$ each. As the original state of the first qubit was $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, measurement of the second qubit hence changes the state of the first — in particular, it "reveals" which state the first qubit was in when we applied U_f, projecting it out of a superposition.

3. We wouldn't want to reset the ancilla by measuring it because we may affect the state of some other qubit which is entangled with it, most likely a superposition of the form $\frac{1}{\sqrt{2}}\sum_{x\in\{0,1\}}|x\rangle$. By changing this state, we may lose the ability to cause interference between the different values of x down the road for instance.

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 $HU_{\overline{f}}H|0\rangle = |f(0) \oplus f(1)\rangle$ up to global phase, where $U_{\overline{f}} : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$.

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

Solution.

1.

$$\begin{aligned}
HH|x\rangle &= H(\frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle) \\
&= \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}H|y\rangle \\
&= \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}[\frac{1}{\sqrt{2}}\sum_{z\in\{0,1\}}(-1)^{yz}|z\rangle) \\
&= \frac{1}{2}\sum_{x,y,z}(-1)^{xy+yz}|z\rangle
\end{aligned}$$

2. Using the fact that y is either equal to c, or $c \oplus 1 = c + 1 \mod 2$, we can write the sum as

$$\begin{aligned}\frac{1}{2}\sum_{x,y}(-1)^{cx+xy}|y\rangle &= \frac{1}{2}\sum_{x}(-1)^{cx+xc}|c\rangle + \frac{1}{2}\sum_{x}(-1)^{cx+x(c+1)}|c\oplus 1\rangle \\ &= \frac{1}{2}\sum_{x}|c\rangle + \frac{1}{2}\sum_{x}(-1)^{x}|c\oplus 1\rangle \\ &= \frac{1+1}{2}|c\rangle + \frac{1+(-1)}{2}|c\oplus 1\rangle \\ &= |c\rangle\end{aligned}$$

3. First observe that $HU_{\tilde{f}}H|0\rangle = \frac{1}{2}\sum_{x,y}(-1)^{f(x)+xy}|y\rangle$. Now writing $f(x) = (1+x)f(0) + xf(1) = f(0) + x(f(0)+f(1))$ we have, up to a global phase of $(-1)^{f(0)}$, exactly the state from part 2, with $c = f(0)+f(1)$. Hence using the result of part 2, $HU_{\tilde{f}}H|0\rangle = (-1)^{f(0)}|f(0)\oplus f(1)\rangle$, or $|f(0)\oplus f(1)\rangle$ up to global phase.

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

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

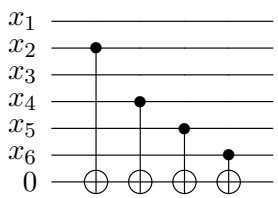
using an oracle $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ (or its phase version, $U_{\tilde{f}} : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$)

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

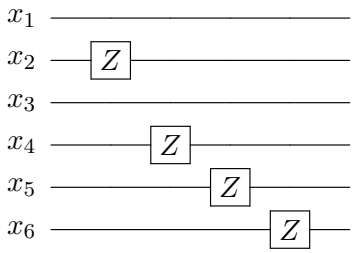
1. Give an implementation of the oracle U_f using $CNOT$ gates.
2. Give an implementation of the oracle $U_{\tilde{f}}$. You may use any of the following: the oracle U_f, H, Z gates or ancillas initialized in $|0\rangle$ or $|1\rangle$.
3. Could the value of s be computed in polynomial time on a classical 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?

Solution.

1.



2.



3. Yes — in the case of U_f, a classical computer could determine the non-zero bits s by checking which bits the $CNOT$ gates are controlled on, and likewise with the Z gates in $U_{\tilde{f}}$.

   Query complexity isn't a great characterization of the problem in this case for a number of different reasons. There's the reason we discussed in class which is that there exists a classical algorithm with both query and real complexity $O(n)$ assuming queries are constant time, but then there's also the reason that this problem implies which is that the correct answer is hidden in plain sight in the construction of the oracle. So even if the BV algorithm gave an exponential separation in query complexity (i.e. if the classical query algorithm took $O(2^n)$ time), there would exist a linear-time classical algorithm which uses the circuit implementation of the quantum query.

   If however we don't assume anything about the structure of the implementation outside of the fact that it is implemented over X, $CNOT$, and Toffoli gates, we could still find the hidden string in polynomial time since the gate set is *purely classical*. Notably, we could simulate the oracle on a classical computer on the n input strings of the form $10\cdots0$, $01\cdots0$, $\ldots$, $00\cdots1$ to find the n bits of s. Better yet, we could execute the oracle *symbolically* in polynomial time to find the unique polynomial representation $f(x) = s_1x_1 \oplus s_2x_2 \oplus \cdots \oplus s_nx_n$ of f and then read out the hidden string.

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.

Solution.

1. For the given function, we have the following uniform superposition of values $|x\rangle|f(x)\rangle$:

$\|x\rangle$	$\|f(x)\rangle$
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|101\rangle$
$\|100\rangle$	$\|001\rangle$
$\|101\rangle$	$\|000\rangle$
$\|110\rangle$	$\|101\rangle$
$\|111\rangle$	$\|010\rangle$

2. Choosing $f(x) = 010$ we now have the state

$$\frac{1}{\sqrt{2}}(|010\rangle + |111\rangle)|010\rangle$$

3. Apply $H^{\otimes 3}$ to the first register we get

$$\begin{aligned} H^{\otimes 3}\frac{1}{\sqrt{2}}(|010\rangle + |111\rangle) &= \frac{1}{4}(|000\rangle + |001\rangle - |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle - |111\rangle \\ &\quad + |000\rangle - |001\rangle - |010\rangle + |011\rangle - |100\rangle + |101\rangle + |110\rangle - |111\rangle) \\ &= \frac{1}{2}(|000\rangle - |010\rangle + |101\rangle - |111\rangle) \end{aligned}$$

4. Taking 2 linearly independent (and hence, non-zero) samples from the state above, we have $|101\rangle$, $|111\rangle$.

5. We need to solve the linear system

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Row reducing, we get

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

and in particular we have the equations $s_1 \oplus s_3 = 0$ and $s_2 = 0$. The only non-trivial solution to the former is $s_1 = s_3 = 1$, hence the hidden string is

$$s = 101$$