# CMPT 476/981: Introduction to Quantum Algorithms
# Assignment 4

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 $\epsilon$. What approximation factor should you choose for each gate?

**Solution.**

1. By calculation:

   $$\begin{aligned} E(U_2U_1, V_2V_1) &= ||U_2U_1 - V_2V_1|| \\ &= ||U_2U_1 - U_2V_1 + U_2V_1 - V_2V_1|| \\ &= ||U_2(U_1 - V_1) + (U_2 - V_2)V_1|| \\ &\leq ||U_2(U_1 - V_1)|| + ||(U_2 - V_2)V_1|| \\ &= ||U_1 - V_1|| + ||U_2 - V_2|| \\ &= E(U_2, V_2) + E(U_1, V_1) \end{aligned}$$

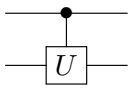
2. Suppose we approximate $U_1 \cdots U_k$ by a sequence of unitary approximations $V_1 \cdots V_k$. Since $E(U_2U_1, V_2V_1) \leq E(U_2, V_2) + E(U_1, V_1)$, we have that

   $$E(U_1 \cdots U_k, V_1 \cdots V_k) \leq E(U_1, V_1) + E(U_2 \cdots U_k, V_2 \cdots V_k) \leq \cdots \leq E(U_1, V_1) + \cdots + E(U_k, V_k)$$

   so $E(U_i, V_i) \leq \epsilon/k$ gives a total error of at most $\epsilon$.

## Question 2 [2 points]: Controlled gates

Recall that a (quantum) controlled unitary is drawn as

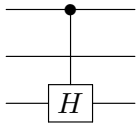



where the dot represents the control, and $U$ is applied only when the control bit is in the state $|1\rangle$.

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




**Solution.**

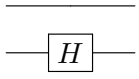
1. Recall that a controlled $U$ gate is defined as a unitary $c-U$ such that

$$c-U|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$$
$$c-U|1\rangle|\psi\rangle = |1\rangle(U|\psi\rangle)$$

   where $|\psi\rangle$ is an arbitrary state of appropriate dimension. Note that $c-U$ is uniquely defined in this way, as $c-U$ is an operator on $\mathbb{C}^2 \otimes \mathbb{C}^{2^n}$ when $U$ is a $2^n$-dimensional unitary, and $\{|0\rangle, |1\rangle\}$ form a basis of $\mathbb{C}^2$. So we need only check that the above expression satisfies these two equations:

$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U)|0\rangle|\psi\rangle = (|0\rangle\langle 0|0\rangle) \otimes (I|\psi\rangle) + (|1\rangle\langle 1|0\rangle) \otimes (U|\psi\rangle) = |0\rangle \otimes |\psi\rangle$$
$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U)|1\rangle|\psi\rangle = (|0\rangle\langle 0|1\rangle) \otimes (I|\psi\rangle) + (|1\rangle\langle 1|1\rangle) \otimes (U|\psi\rangle) = |1\rangle \otimes (U|\psi\rangle)$$

2. Observe that the circuit




   mathematically corresponds to the operator $I \otimes H$. So the circuit in question is a controlled

$I \otimes H$ gate, which has matrix

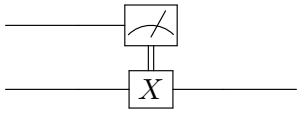
$$|0\rangle\langle 0| \otimes (I \otimes I) + |1\rangle\langle 1| \otimes (I \otimes H) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$$

## Question 3 [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.

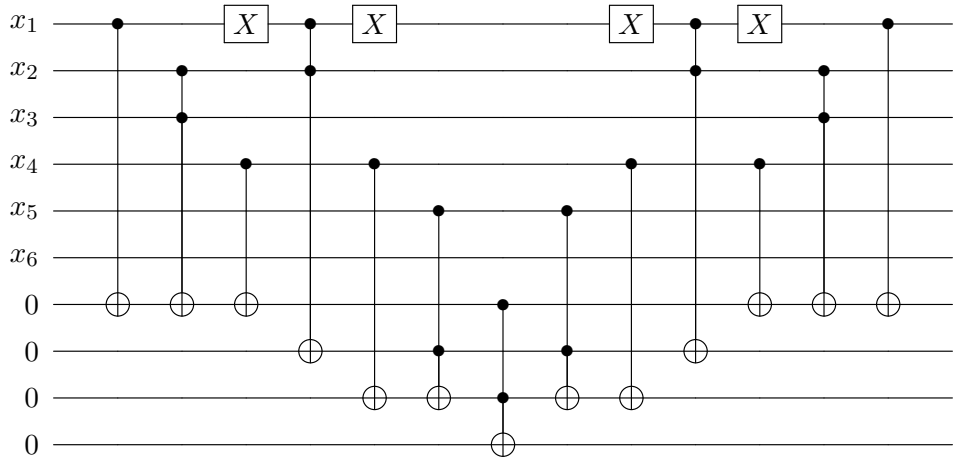
## Question 4 [3 points]: Reversible circuits

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.

**Solution.**




## Question 5 [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 6 [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 $s = 010111$.

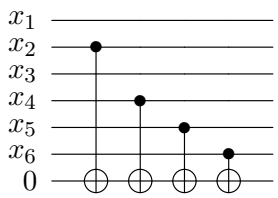
1. Give an implementation of the oracle $U_f$ using $CNOT$ gates.

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 $|1\rangle$.

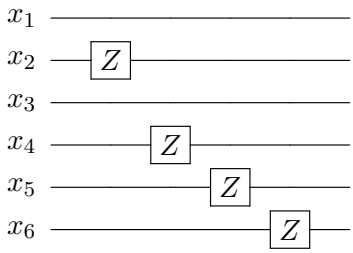
3. Could the value of $s$ be computed in polynomial time on a classical computer from your implementation of either $U_f$ or $U_{\tilde{f}}$? Do you think query complexity is a good characterization of the problem in this case? What if instead $U_f$ was any polynomial-sized oracle for $f$ over the gate 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, with the simplest analysis we can't solve the problem efficiently from the implementation of the oracle since it doesn't necessarily reveal the bit string. We can note that the oracle suffices to efficiently (in the oracle size) compute a symbolic representation of $f$ since the gate involved are strictly classical, though it may in general be possible that $f(x) = x \cdot s$ has some other symbolic representation which again doesn't explicitly reveal $s$.

## Question 7 [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 $s$, 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

$$s=101$$