COL863: Quantum Computation and Information
Homework: 01

1. $\mathsf{P} = \mathsf{NP}$ has a lot of interesting consequences. One consequence is that one-way functions do not exist if $\mathsf{P} = \mathsf{NP}$. This is significant since much of known cryptography is based on the existence of one-way functions. In other words, Cryptography is built on an assumption that is stronger than $\mathsf{P} \neq \mathsf{NP}$. In this question you are asked to show this formally. First, we look at the definition of one-way functions.

   Definition 1.0.1 (One Way Function) *A function $f : \{0,1\}^* \to \{0,1\}^*$ is called a one way function if the following two conditions hold:*

   (a) (Easy to compute:) There exists a polynomial-time algorithm M_f computing f; that is, $M_f(x) = f(x)$ for all x.

   (b) (Hard to invert:) For every PPT algorithm A, there exists a negligible function negl (a function that is smaller than any polynomial) such that

   $$\mathbf{Pr}[Invert_{A,f}(n) = 1] \leq negl(n)$$

   Where $Invert_{A,f}(n)$ denotes the following experiment:
   $Invert_{A,f}(n)$

   - Choose input $x \leftarrow \{0,1\}^n$. Compute $y = f(x)$.

   - Execute A with inputs 1^n and y. Let x' be the output of A.

   - The output of the experiment is defined to be 1 if $f(x') = y$, and 0 otherwise.

   Argue that if $\mathsf{P} = \mathsf{NP}$, then one way functions do not exist.
   (*I gave this question since this was raised in the class discussions. You only need to argue at a very high level.*)

2. Can the following two-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ be represented as $(\alpha|0\rangle+\beta|1\rangle)(\alpha'|0\rangle+\beta'|1\rangle)$?

3. Can there exist a single qubit gate with the following truth table? Give reasons.

Input	Output
$\|0\rangle$	$\frac{\sqrt{3}}{2}\|0\rangle + \frac{1}{2}\|1\rangle$
$\|1\rangle$	$\frac{1}{2}\|0\rangle + \frac{\sqrt{3}}{2}\|1\rangle$

4. Show that there exist a single qubit gate with the following truth table? Give the matrix representation of such a gate.

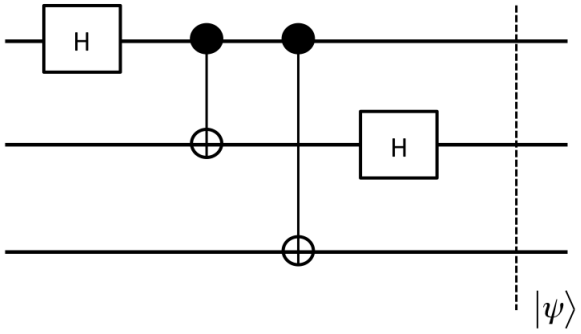
Input	Output
$\|0\rangle$	$\frac{\sqrt{3}}{2}\|0\rangle - \frac{1}{2}\|1\rangle$
$\|1\rangle$	$\frac{1}{2}\|0\rangle + \frac{\sqrt{3}}{2}\|1\rangle$

5. Draw the classical circuit for computing the Boolean function $f : \{0,1\}^2 \to \{0,1\}$ given by the following truth table.

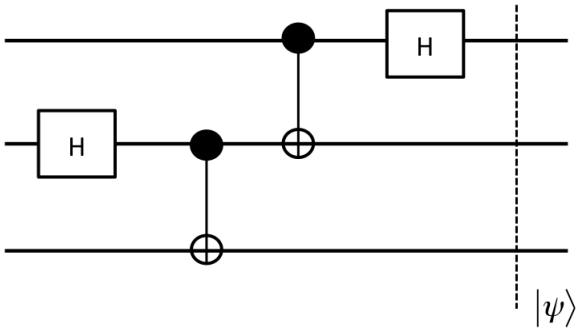
x	$f(x)$
00	1
01	0
10	1
11	0

Give the Quantum analogue of your classical circuit using Toffoli gates.

6. Output $|\psi\rangle$ when the input to the circuit is $|000\rangle$. Output $|\psi\rangle$ when the input is $[\alpha\,|0\rangle + \beta\,|1\rangle]\,|00\rangle$.

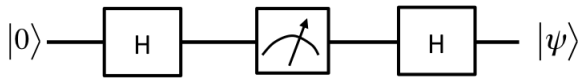


7. Output $|\psi\rangle$ when the input to the circuit is $|000\rangle$. Output $|\psi\rangle$ when the input is $[\alpha\,|0\rangle + \beta\,|1\rangle]\,|00\rangle$.

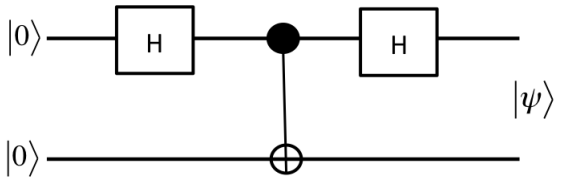


8. Can you use a single qubit as a source of randomness? How?

9. In this problem, we will discuss the *principle of deferred measurement*. The main idea is that any (randomized) computation that a quantum circuit can perform by making *intermediate* measurements can also be performed by a slightly modified circuit that does *all* measurements at the very end. Let us try to understand the subtleties of this point (which we did not discuss in the class). Consider the following single qubit circuit:



What is the output $|\psi\rangle$? A bit of thinking tells you that the output is not a "pure" state but a randomized state. That is, $|\psi\rangle$ is $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$. This is because the measurement collapses the state of the qubit to either $|0\rangle$ or $|1\rangle$. Now, you can imagine a multiple-qubit circuit that uses intermediate measurements. The output state of the multiple qubit system will be a *mixture* of states. This can be useful in a lot of computational settings where it can be interpreted as randomized computation. It would be theoretically much simpler if all the measurements were taken at the end of the circuit (as we have seen in all examples discussed in the class). This is actually possible by using some *ancilla* input qubits. Here I will only give you the main idea and then ask you to fill out the details for the general problem. Let us go back to our previous example. Suppose we want to simulate this circuits behaviour without making the intermediate measurement. Consider the following circuit:



Suppose we make a measurement on only the first qubit at the end. Does the measurement behaviour of this qubit remains that same as in the previous case where we also made an intermediate measurement? Use this idea to convince yourself of the principle of deferred measurements.