Quantum Computation 101 for Physicists

Home exercise 4

1. Suppose we have a 2-bit input $x = x_0x_1$, and a 1-qubit unitary U_x that adds a phase as follows:
$$U_x|b\rangle = (-1)^{x_b}|b\rangle.$$
   (a) Suppose we run the 1-qubit circuit $HU_xH|0\rangle$ and then measure in the computational basis. What is the probability distribution on the measurement output, as a function of x?

   (b) Suppose now that the query leaves some mess on an auxiliary bit,
$$U'_x|b0\rangle = (-1)^{x_b}|bb\rangle.$$
   If we now apply $H_0(U'_x)_0H_0|0,0\rangle$ and measure qubit 1 in the computational basis, what is the probability distribution on the measurement output now?

   Note: this question is here to demonstrate the importance of cleaning up auxiliary qubits when performing calculations (the uncompute trick we saw in class). In other words, it displays the effect of entangling a qubit to its environment.

2. In class we saw that if we have cU, we can create ccU. Practically, 2-qubit gates are much harder to implement than 1-qubit gates, and in many implementations it's preferred to implement only one 2-qubit gate and do the rest with 1-qubit gates (we saw in class a universal set which shows that this is possible). Now you will show how to implement a quantum gate cU using 2 $cNOT$s and 1-qubit gates.

   (a) Use the representation we saw on the first week for a 1-qubit unitary, $U(\varphi, \hat{n}) = \frac{1}{2}(\cos\frac{\varphi}{2}\mathbb{I} + i\sin\frac{\varphi}{2}\hat{n}\cdot\vec{\sigma})$, to show that $UXU^\dagger = (\vec{a}\cdot\vec{\sigma})$, and find the vector $\vec{a}$.
   Use $(\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = \vec{a}\cdot\vec{b}\mathbb{I} + i(\vec{a}\times\vec{b})\cdot\vec{\sigma}$. It is helpful to denote $X = \hat{d}\cdot\vec{\sigma}$, where $\hat{d} = (1, 0, 0)$.

   (b) Show that any operator $U(\vec{n}, \varphi)$ can be achieved by choosing the right V, W unitaries such that $U = VXV^\dagger WXW^\dagger$.Use $(\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = \vec{a}\cdot\vec{b}\mathbb{I} + i(\vec{a}\times\vec{b})\cdot\vec{\sigma}$ again, and no need for a strict rigorous proof, a hand-waving justification (such as counting the necessary degrees of freedom in the requirement) is enough.

   (c) Use (b) to construct circuit that implements a general controlled-U using two cX gates and 1 - qubit gates.

3. Quick reminder of Simon's algorithm (2.5 in Mermin's book):

   (a) We have a function f that has some period a, i.e. $f(x) = f(y) \iff y = x \oplus a$. We want to find a.

   (b) In class we saw that if we have a unitary operator such that $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, we can get the state $\frac{1}{2^{n/2}}\sum_{i=1}^{2^n}|i\rangle|f(i)\rangle$.

   (c) We now measure the second register to get $\frac{1}{\sqrt{2}}(|i_0\rangle + |i_0 \oplus a\rangle)$ for some i_0 our function collapsed into.

   (d) We apply $H^{\otimes n}$ to get $\frac{1}{2^{\frac{n+1}{2}}}\sum_{y=0}^{2^n-1}((-1)^{i_0\cdot y} + (-1)^{(i_0\oplus a)\cdot y})|y\rangle = \frac{1}{2^{\frac{n-1}{2}}}\sum_{y\cdot a=0}(-1)^{i_0\cdot y}|y\rangle$.

   (e) By measuring y we can learn a little bit about a,and in class we saw that we need on average a linear number of such repetitions until we learn a.

   Our question for now is this: In stage (c), when we measure the last $n-1$ qubits with the value $f(i_0)$, we don't use it at all in the algorithm. Show that we can in fact perform the algorithm without measuring the last $n-1$ qubits at any stage of the algorithm.