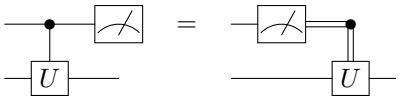
Dropbox submission folder link: https://www.dropbox.com/request/oUv9nYB3HrbH4fSlhJHx

Problem Set 4: Quantum Circuits and Algorithms

1. One of the principles of the quantum circuit model is that all of the measurements may be pushed to the end of the quantum computation. Show that this is true for controlled operations. That is, show that the following two circuits produce identical outcomes:



(1)

That is: the quantum C-U operation followed by measurement is equivalent to measurement followed by the classical conditional application of U. "Identical outcomes" refers to measurement probabilities and system state after the circuit.

2. We know that we can implement any ideal quantum evolution U to accuracy ϵ by a circuit $\tilde{U}$ built from a universal gate set. That is, for any $\epsilon > 0$, we can find $\tilde{U}$ such that $\left\|U - \tilde{U}\right\|_{op} \leq \epsilon$. The output of a quantum computation comes from the final complete orthogonal measurement in the computational basis, however. What we should really check is that the probability of obtaining outcome x in the ideal case $p(x)$ is close to the probability in the non-ideal case $\tilde{p}(x)$.

   The L^1 distance between two probability distributions is defined to be

$$d(p, \tilde{p}) = \|p - \tilde{p}\|_1 = \sum_x |p(x) - \tilde{p}(x)| \tag{2}$$

   Show that $\left\|U - \tilde{U}\right\|_{op} \leq \epsilon$ implies that the distribution of the measurement outcomes is close in the L^1 norm: $d(p, \tilde{p}) \leq 2\epsilon$ (hint: you may need Cauchy-Schwarz.)

3. For a database with r marked items out N total, the Grover iteration produces a rotation by an angle θ such that $\sin\theta = \sqrt{\frac{r}{N}}$. In order to get a high probability of measuring a marked state, the optimal algorithm applies $T \approx \frac{\pi}{4\theta}$ iterations. Suppose we know that the number of marked states $r < \sqrt{N}$, but are unsure about its precise value so we don't know what T to pick. Show that for any fixed $1 < r < \sqrt{N}$, if we randomly choose T uniformly between 0 and $\sqrt{N} - 1$, the probability of measuring a marked state is at least 1/8 (for N large enough).

4. The Grover reflection relies on the n-bit controlled X gate, $C^{n-1}(X)$. In order for Grover to be efficient, we need $C^{n-1}(X)$ to be efficiently constructable (not exponential in n).

   (a) Show that $C^{n-1}(X)$ can be constructed using $2n - 5$ $C^2(X)$ (Toffoli) gates using $n - 3$ scratch bits which are initially 0 and returned to 0 at the end of the circuit.

   (b) Show that $C^{n-1}(X)$ can be constructued using $4n - 12$ $C^2(X)$ gates using $n - 3$ scratch bits which are reset by the end of the circuit but need not be initialized to 0.

(Continued on next page...)

5. **An exactly universal quantum gate set.**

NOTE: in this problem's notation $\Lambda(X)$ is a controlled X gate (we have been calling this $C(X)$).

The purpose of this exercise is to complete the demonstration that the controlled-NOT gate $\Lambda(\boldsymbol{X})$ and arbitrary single-qubit gates constitute an exactly universal set.

a) If $\boldsymbol{U}$ is any unitary 2×2 matrix with determinant one, find unitary $\boldsymbol{A}, \boldsymbol{B}$, and $\boldsymbol{C}$ such that

$$\boldsymbol{ABC} = \boldsymbol{I} \tag{5.113}$$

$$\boldsymbol{AXBXC} = \boldsymbol{U}. \tag{5.114}$$

Hint: From the Euler angle construction, we know that

$$\boldsymbol{U} = \boldsymbol{R}_z(\psi)\boldsymbol{R}_y(\theta)\boldsymbol{R}_z(\phi), \tag{5.115}$$

where, *e.g.*, $\boldsymbol{R}_z(\phi)$ denotes a rotation about the z-axis by the angle ϕ. We also know that, *e.g.*,

$$\boldsymbol{X}\boldsymbol{R}_z(\phi)\boldsymbol{X} = \boldsymbol{R}_z(-\phi). \tag{5.116}$$

b) Consider a two-qubit *controlled phase gate* which applies $\boldsymbol{U} = e^{i\alpha}\mathbf{1}$ to the second qubit if the first qubit has value $|1\rangle$, and acts trivially otherwise. Show that it is actually a one-qubit gate.

c) Draw a circuit using $\Lambda(\boldsymbol{X})$ gates and single-qubit gates that implements $\Lambda(\boldsymbol{U})$, where $\boldsymbol{U}$ is an arbitrary 2×2 unitary transformation.

In lecture we have shown that the gate set $\{\Lambda(\mathbf{U})\}$ is exactly universal. Therefore this problem proves that $\{\Lambda(\mathbf{X})\}$ together with single-qubit gates are an exactly universal set.