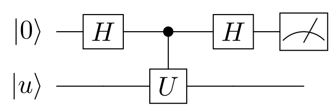
2.111/8.370/18.435 Problem Set 9 Solutions

Due: December 3, 2015

1. **(Poor man's phase estimation) Consider the following circuit**



where $U|u\rangle = e^{i\phi}|u\rangle$.

(a) We measure the top register in the computational basis. Find the probability of obtaining $|1\rangle$.

(b) How many times do we have to repeat to estimate ϕ to accuracy ϵ?

(a) The circuit does the following:

$$|0\rangle|u\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle|u\rangle) \xrightarrow{C-U} \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + e^{i\phi}|1\rangle|u\rangle) \xrightarrow{H\otimes I} e^{i\phi/2}(\cos\frac{\phi}{2}|0\rangle|u\rangle - i\sin\frac{\phi}{2}|1\rangle|u\rangle).$$

The probability of measuring $|1\rangle$ is $|-i\sin\frac{\phi}{2}|^2 = \sin^2\frac{\phi}{2}$.

(b) Each repetition of the above procedure is equivalent to flipping a $\{p_1 = \sin^2\frac{\phi}{2}, p_0 = \cos^2\frac{\phi}{2}\}$ biased coin.

Suppose we do it independently for N times. The sum of outcomes s follows a binomial distribution with mean $\bar{s} = Np_1$ and variance $\sigma^2 = Np_1(1-p_1)$. We output $\tilde{p}_1 = s/N$, and with 68% confidence this estimation falls within 1σ about the true value of p_1, i.e.,

$$|p_1 - \tilde{p}_1| \le \sqrt{\frac{p_1(1-p_1)}{N}}.$$

(You can choose 2σ: 95%, 3σ: 99.7%, ..., depending on the confidence level you want.)

Notice that

$$|p_1 - \tilde{p}_1| = |\sin^2\frac{\phi}{2} - \sin^2\frac{\tilde{\phi}}{2}| = \frac{1}{2}\sin\phi|\phi - \tilde{\phi}| + O(|\phi - \tilde{\phi}|^2).$$

We want $|\phi - \tilde{\phi}| \le \epsilon$. So up to leading order, we need

$$\sqrt{\frac{p_1(1-p_1)}{N}} \le \frac{1}{2}\sin\phi\epsilon.$$

Plugging in $p_1 = \sin^2\frac{\phi}{2}$, we obtain

$$N \ge \frac{\sin^2\frac{\phi}{2}\cos^2\frac{\phi}{2}}{\sin^2\phi\epsilon^2} = \frac{1}{\epsilon^2}.$$

(For $c\sigma$ confidence level, $N \ge c^2/\epsilon^2$.)

2. **Show that the following controlled-U operation**

$$V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

is unitary.

$$V^\dagger = |0\rangle_A\langle 0| \otimes I_B + |1\rangle_A\langle 1| \otimes U_B^\dagger.$$

$$V^\dagger V = |0\rangle_A\langle 0| \otimes I_B + |1\rangle_A\langle 1| \otimes U_B^\dagger U_B = (|0\rangle_A\langle 0| + |1\rangle_A\langle 1|) \otimes I_B = I_{AB}.$$

3. **Show that $|i\rangle \mapsto (-1)^{f(i)}|i\rangle$ where $f(i) = \delta_{iw}$ is performed by $U_G = I - 2|w\rangle\langle w|$.**

$$U_G|i\rangle = (I - 2|w\rangle\langle w|)|i\rangle = |i\rangle - 2\langle w|i\rangle|w\rangle = |i\rangle - 2\delta_{iw}|w\rangle = (-1)^{\delta_{iw}}|i\rangle.$$

4. **Define $|\vec{1}\rangle = \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|i\rangle, U_{\vec{1}} = I - 2|\vec{1}\rangle\langle\vec{1}|$. Take $n = 4, w = 2$. Compute $U_{\vec{1}}U_G|\vec{1}\rangle$. Can we find w from this?**

   When $n = 4$ and there is only one w, $\langle\vec{1}|w\rangle = \frac{1}{2}$. Thus

$$U_G|\vec{1}\rangle = (I - 2|w\rangle\langle w|)|\vec{1}\rangle = |\vec{1}\rangle - |w\rangle.$$

$$U_{\vec{1}}U_G|\vec{1}\rangle = (I - 2|\vec{1}\rangle\langle\vec{1}|)(|\vec{1}\rangle - |w\rangle) = -|\vec{1}\rangle - |w\rangle + |\vec{1}\rangle = -|w\rangle.$$

   Therefore we can find $|w\rangle$ with one query to the oracle U_G when $n = 4$. (It doesn't matter what w is.)