University of California at San Diego – Department of Physics – TA: Shauna Kravec

Quantum Mechanics C (Physics 130C) Winter 2015
Worksheet 8

Announcements

- The 130C web site is:

  http://physics.ucsd.edu/∼mcgreevy/w15/ .

  Please check it regularly! It contains relevant course information!

  This week we'll be discussing phase estimation, order finding, and factoring integers.

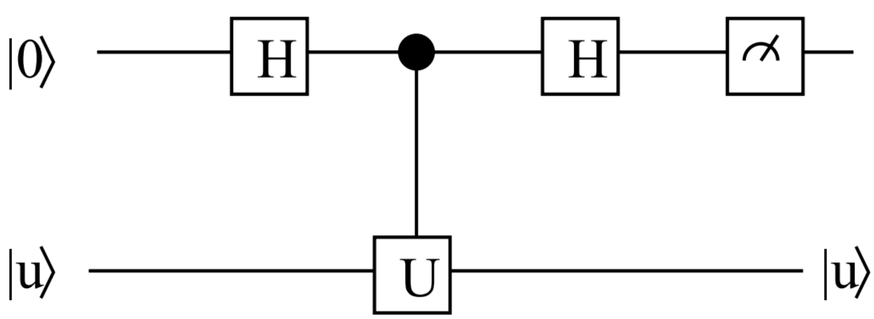
Problems

1. **Phase Estimation**

   Consider a two-qubit system and a unitary operator U with eigenvector $|u\rangle$

   By unitarity we know that the eigenvalue has the form $U|u\rangle = e^{\mathbf{i}2\pi\theta}|u\rangle$ for some $\theta \in (0, 1)$ which we would like to determine. Challenge: this eigenvalue has norm 1.

   So! Consider the following quantum circuit:



   where $\hat{H} = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle-|1\rangle}{\sqrt{2}}\langle 1|$ is the Hadamard gate and the second line is the Control-U operator $CU = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$

   (a) Write down the wavefunction for the qubit pair after each step in the circuit

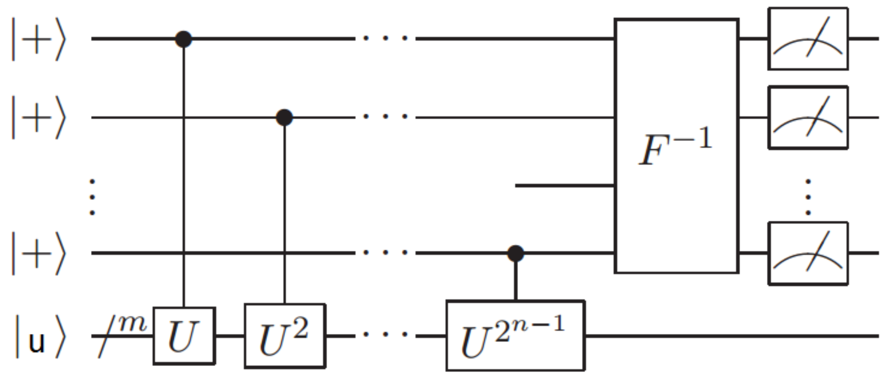
   (b) After the circuit is applied show that the probability of measuring the first qubit to be $|0\rangle$ is $p = \cos^2(\pi\theta)$. Note the answer if $\theta = \frac{z}{2^1}$ for some integer z.

   So by estimating p we can determine θ perfectly in the special case. More generally we could crudely estimate it up to the ambiguity of $\cos^2(\pi\theta) = \cos^2(\pi(1-\theta))$

   Can we do better? Suppose instead of two qubits we have $n+1$ and an input state $|In\rangle = |00\cdots 0\rangle|u\rangle$

(c) Apply the Hadamard gate to each of the first n qubits. What is the result?

Now consider this improved phase estimation circuit



where F^{-1} is the *quantum* inverse Fourier transformation and the other gates are CU^{2^j} gates applied incrementally to the first n qubits and $j \in \{0, 1, \cdots, n-1\}$

(d) Before the F^{-1}, what is the state of the system? (Hint: What is $CU^{2^j}|+\rangle|u\rangle$?)

Now we need to tackle this Fourier transformation. For our purposes it is sufficient to define it by

$$F|x\rangle = \frac{1}{\sqrt{N}} \sum_y e^{\frac{2\pi \mathbf{i} xy}{N}} |y\rangle \tag{1}$$

(e) Show that for $\theta = \frac{z}{N}$ for some integer z that the output of the phase estimator circuit gives probability 1 to determine z correctly when measuring the control qubits in the computational basis. What's the probability more generally?

2. **Order Finding**

Suppose I want to find a factor of an integer N. We'll pick a random integer $0 < a < N$ such that $\text{GCD}[a, N] = 1$ and determine the integer r such that $a^r = 1 \text{ mod } N$

Without proof, I claim that with $> \frac{1}{2}$ probability r is even and $a^{\frac{r}{2}} \neq \pm 1 \text{ mod } N$

Given this N divides $a^r - 1$ which imples N divides $(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$ but not each independently. Thus atleast one of $(a^{\frac{r}{2}} \pm 1)$ contains a factor of N which we pick out by computing $\text{GCD}[a^{\frac{r}{2}} + 1, N]$

(a) Consider the case of $N = 15$ and $a = 4$.

Hopefully the above convinces you that order finding is the thing to do. To accomplish this consider the following unitary operator:

$$U_a|x\rangle = |ax \text{ mod } N\rangle \quad 0 \leq x \leq N \tag{2}$$

(b) Show that $\lambda_k = e^{\frac{2\pi \mathbf{i} k}{r}} \equiv \omega^k$ are eigenvalues of U_a for $0 \leq k < r$

(c) Show that $|\phi_k\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{\frac{-2\pi \mathbf{i} k \ell}{r}} |a^\ell \text{ mod } N\rangle$ are eigenvectors of U_a

But now suppose you were handed $|\phi_k\rangle$ delicately prepared. We could use the phase estimation circuit above to estimate $\theta = \frac{k}{r} \approx \frac{z}{2^n}$ which, as long as k and r are not relatively prime[1], we get r!

Now it is a justified complaint that, without knowing r, constructing $|\phi_k\rangle$ would be impossible.

However, superpositions of these eigenvectors aren't hard to make.

(d) Show $|1\rangle = \frac{1}{\sqrt{r}} \sum_k |\phi_k\rangle$

So using $|1\rangle$ as our input our measurement still produces, with good probability, a rational approximation to $\frac{k}{r}$ but for some uniformly random k. Is it good enough?

As it turns out yes! But that's beyond today.

[1] For large r this get's unlikely, another claim without proof.