Ph/CS 219, Fall 2006
Quantum Computation
Prof. Alexei Kitaev

Problem set #4
Due Monday, December 4, 2006

4.1 Quantum circuit design.

a) Express the operator $\Lambda^2(-1)$ as a product of $\exp\bigl(i\frac{\pi}{4}\sigma_1^z\bigr)$, $\exp\bigl(i\frac{\pi}{4}\sigma_2^z\bigr)$, and $\exp\bigl(i\frac{\pi}{4}\sigma_1^z\sigma_2^z\bigr)$ up to an overall phase. Each of the above elementary operators may be use multiple times. (Note that $\exp\bigl(i\frac{\pi}{4}\sigma^z\bigr) \equiv \Lambda(-i)$ up to an overall phase.)

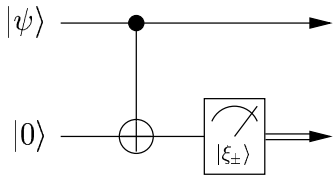
b) Construct an exact realization of the operator $\Lambda^2(i)$ using the following set of gates: H (the Hadamard gate), $\Lambda(\sigma^x)$ (the controlled NOT), and $\Lambda\bigl(e^{i\pi/4}\bigr)$. For simplicity, you may assume that all the gates come with there inverses, i.e., $\Lambda\bigl(e^{-i\pi/4}\bigr)$ is also available.

4.2 Computation by measurement. The standard scheme of quantum computation implies that all bits are quantum, all gates are unitary, and a measurement occurs at the very end. In practice, however, it may be convenient to supplement a "quantum CPU" with a classical co-processor and let them communicate. More specifically, we allow qubit measurements in the middle of computation. The measurement outcomes are processed classically, and the computed classical value may influence the choice of the quantum gate to be executed next. This model is called *adaptive quantum computation*. Let us consider a simple example.

Suppose we can perform the gates $\Lambda(\sigma^x)$, σ^x, σ^y, σ^z and measure a qubit with respect to this basis:

$$|\xi_+\rangle = \frac{1}{\sqrt{2}}\Bigl(|0\rangle + e^{i\varphi}|1\rangle\Bigr), \qquad |\xi_-\rangle = \frac{1}{\sqrt{2}}\Bigl(|0\rangle - e^{i\varphi}|1\rangle\Bigr). \tag{1}$$

Using this set of elementary operations, implement the unitary operator $\Lambda\bigl(e^{-i\varphi}\bigr)$. **Hint:** Consider the following circuit:



Show that for an arbitrary initial state $|\psi\rangle$, both possible measurement outcomes ("+" and "−") occur with probability 1/2. For each of the outcomes, find the final state of the first qubit.[1] Choose a supplementary operation to be executed next, so that the net result is always the application of $\Lambda\bigl(e^{-i\varphi}\bigr)$.

4.3 Quantum Zeno effect: patience is golden. Consider the Grover search algorithm. Let U_f be the quantum oracle corresponding to the function $f : \{1, \ldots, N\} \to \{0, 1\}$, i.e.,

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle. \tag{2}$$

[1] In this calculation, we assume that the initial state is known, but this may not be true when the circuit is operated. Note that the measurement reveals no information about $|\psi\rangle$.

We start with the state $|+\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$ and repeatedly apply the Grover operator

$$R = -U_+ U_f, \qquad \text{where } U_+ = 1 - 2|+\rangle\langle +|. \tag{3}$$

a) Write an explicit expression for the quantum state after k iterations, assuming that the search problem has M solutions ($M \neq 0$, $M \neq N$). Use this notation:

$$|\text{good}\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle, \qquad |\text{bad}\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle. \tag{4}$$

After how many steps the state is close to $|\text{good}\rangle$ if $M \ll N$?

b) Now suppose that we are impatient to see if the result is ready. We measure the value of the oracle function $f(x)$ on the initial state and after each iteration. If the outcome is 1, we can further measure x and be sure that it is one of the solutions, otherwise we perform a Grover iteration and measure $f(x)$ again. How many steps (in the average) does it take to find a solution this way?

4.4 Hidden shift problem. This problem appears to be similar to period finding, yet it is much harder. (It is actually equivalent to the hidden subgroup problem in a so-called *dihedral group*, which is non-Abelian.) Consider two functions, $f_0, f_1 : \mathbb{Z}_N \to \{0,1\}^m$. Each function takes on distinct values as the argument runs over its domain (i.e., $f_a(x) = f_a(y)$ if and only if $x = y$), but the two functions are related as follows:

$$f_0(x) = f_1(x + \omega). \tag{5}$$

Here, ω is an unknown element of the group $\mathbb{Z}_N$. The goal is to find it by querying this quantum oracle:

$$\widehat{f_\oplus}|a, x, u\rangle = |a, x, u \oplus f_a(x)\rangle, \tag{6}$$

where $\oplus$ denotes the bitwise XOR on m bits.

Let us try the following method. We create the state

$$|\xi\rangle = \frac{1}{\sqrt{2N}} \sum_{a=0,1} \sum_{x \in \mathbb{Z}_N} |a, x, 0^m\rangle, \tag{7}$$

let the oracle compute $f_a(x)$, after which we discard the computed value. Thus we obtain this mixed state:

$$\rho = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} |\psi_x\rangle\langle\psi_x|, \qquad \text{where} \quad |\psi_x\rangle = \frac{1}{\sqrt{2}}\big(|0, x\rangle + |1, x+\omega\rangle\big). \tag{8}$$

a) Write the state ρ in the Fourier basis, i.e., represent it in the form

$$\rho = \sum_{q,q'} A(q,q') \otimes \big(|\xi_q\rangle\langle\xi_{q'}|\big), \qquad \text{where } |\xi_q\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} e^{iqx}|x\rangle, \quad q = \frac{2\pi y}{N}, \ \ y \in \mathbb{Z}_N. \tag{9}$$

(Here, $A(q,q')$ is some operator acting on the first qubit.)

b) Now we measure the first qubit in the basis $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big)$. We also measure the momentum q. Show that the outcome (α, q) occurs with the following probabilities:

$$p(+,q) = \frac{1+\cos q\omega}{2N}, \qquad p(-,q) = \frac{1-\cos q\omega}{2N}. \tag{10}$$

c) Let $n = \lceil \log_2 N \rceil$. Show that the unknown parameter ω can be found with $O(n)$ queries to the oracle and exponential *classical* postprocessing. (The algorithm must produce the correct result with probability at least 2/3.) **Hint:** We sample $k = O(\log n)$ pairs according to the above distribution. Then we try every possible value of ω and find the best fit.