# UNM Physics 452/581: Introduction to Quantum Information, Problem Set 5, Fall 2007

Instructor: Dr. Landahl
Issued: Tuesday, October 9, 2007
Due: Thursday, October 18, 2007

Do all of the problems listed below. Hand in your problem set at the beginning of class on the desk at the front of the classroom or after class in the box in the Physics and Astronomy main office by 5 p.m. **Please put your name and/or IQI number number on your assignment**, as well as the course number (Physics 452/581). Please show all your work and write clearly. Credit will be awarded for clear explanations as much, if not more so, than numerical answers. Avoid the temptation to simply write down an equation and move symbols around or plug in numbers. Explain what you are doing, draw pictures, and check your results using common sense, limits, and/or dimensional analysis.

### 5.1. Exact Grover for 1 in $N$ unordered search

For the unordered search problem on $N$ items where exactly one item (the "winner" $w$) is promised to be marked, the Grover operator is

$$G := -WZ_0WZ_X, \tag{1}$$

where

$$n := \lceil \log_2 N \rceil \qquad Z_0 := I - 2|0\rangle\langle 0| \tag{2}$$

$$W := H^{\otimes n} \qquad Z_X := I - 2|w\rangle\langle w|. \tag{3}$$

(Note that $Z_0$ and $Z_X$ are $n$-qubit operators.)

We saw in class that it was convenient for the "geometric interpretation" of Grover's algorithm to introduce an angle $\alpha$ defined as

$$\cos\alpha := \sqrt{1 - \frac{1}{N}} \qquad \sin\alpha := \sqrt{\frac{1}{N}} \tag{4}$$

so that we could write

$$|s\rangle := W|0\rangle^{\otimes n} \tag{5}$$

$$= \cos\alpha|w^\perp\rangle + \sin\alpha|w\rangle, \tag{6}$$

where $|w^\perp\rangle$ is a state orthogonal to $|w\rangle$.

Applying the Grover operator $k$ times to the state $|s\rangle$ yields

$$G^k|s\rangle := \cos((2k+1)\alpha)|w^\perp\rangle + \sin((2k+1)\alpha)|w\rangle. \tag{7}$$

If

$$\overline{k} := \frac{\pi}{4\alpha} - \frac{1}{2} \tag{8}$$

were an integer, then choosing $k = \overline{k}$ would yield the marked state $|w\rangle$ *exactly*.

($a$) Evaluate $\overline{k}$ for $N = 1, 2, 3, 4$. Are any of these integers?

For most values of $N$, $\overline{k}$ is not an integer. As argued in class, by choosing $k$ to be the nearest integer above or below $\overline{k}$, the result will be state with a large amplitude on the state $|w\rangle$. Although this doesn't yield $|w\rangle$ exactly, by repeating the operation $G^k|s\rangle$ a constant number of times $m$, the probability of not finding $w$ can be suppressed to $\mathcal{O}(N^{-m})$.

With just a little modification, Grover's algorithm can be made exact when the number of marked items is known. This is somewhat surprising, as classical randomized algorithms for the unordered search problem can't be derandomized by using this information. The purpose of this problem is to work through such a modification. (Different modifications having the same effect are also known.)

Consider a one-qubit gate $B$ whose action on the state $|0\rangle$ is

$$B|0\rangle = \sqrt{1 - Na}|0\rangle + \sqrt{Na}|1\rangle \tag{9}$$

for some real number $a$.

($b$) What range of values for $a$ makes $B$ a valid unitary operator? (*Hint*: It must be true that $\|B|0\rangle\| = 1$.)

($c$) The action of $B$ must also be defined on the state $|1\rangle$. Any such action that preserves the unitarity of $B$ is called a *unitary extension* of the action defined in Eq. 9. Give an example of a unitary extension of $B$. (*Hint*: If your answer is correct, then $\langle i|B^\dagger B|j\rangle = \langle i|j\rangle$ for all $i$ and $j$.)

Using the operator $B$, one can define an "extended" Grover operator on $(n + 1)$ qubits as

$$G' := -W'Z_0'W'Z_X', \tag{10}$$

where

$$|w'\rangle := |1\rangle|w\rangle \qquad Z_0' := I - 2|0\rangle\langle 0| \tag{11}$$

$$W' := B \otimes H^{\otimes n} \qquad Z_X' := I - 2|w'\rangle\langle w'|. \tag{12}$$

Moreover, we can give this operator a "geometric interpretation" by defining a new angle $\alpha'$ via

$$\cos\alpha' := \sqrt{1 - a} \qquad \sin\alpha' := \sqrt{a}. \tag{13}$$

(*d*) Show that the state $|s'\rangle := W'|0\rangle^{\otimes(n+1)}$ can be written as

$$|s'\rangle = \cos\alpha'|w'^{\perp}\rangle + \sin\alpha'|w'\rangle, \tag{14}$$

where $|w'^{\perp}\rangle$ is a state orthogonal to $|w'\rangle$.

(*e*) Show that $Z'_X$ is the controlled phase-oracle gate. *I.e.*, show that $Z'_X = \Lambda(Z_X)$.

Parts (*b*), (*c*), and (*e*) demonstrate that if one can implement $G$ on $n$ qubits, then one can implement $G'$ on $(n+1)$ qubits for any $\alpha'$ in the range specified in part (*b*). Moreover, the geometric interpretation provided by part (*d*) shows that applying the extended Grover operator $k$ times to the state $|s'\rangle$ yields

$$(G')^k|s\rangle := \cos((2k+1)\alpha')|w'^{\perp}\rangle + \sin((2k+1)\alpha')|w'\rangle. \tag{15}$$

It seems as though we are in the same situation as before—$k$ will not generally be an integer, so we cannot obtain $|w'\rangle$ (and hence $w$) exactly. However, $\alpha'$ is a free parameter, so we can choose it so that an integral choice for $k$ *will* yield $|w'\rangle$ exactly. For example, consider the choice

$$\alpha' := \frac{\pi}{4\left\lceil \overline{k} \right\rceil + 2}, \tag{16}$$

where $\overline{k}$ is given by Eq. 8.

(*f*) Verify that this choice of $\alpha'$ leads to a value for $a$ that is within the valid range you specified in part (*b*).

(*g*) Show that for $k = \left\lceil \overline{k} \right\rceil$ and the $\alpha'$ from Eq. 16 that $(G')^k|s'\rangle$ yields $|w'\rangle$ with certainty.

Note that this $k = \mathcal{O}(\sqrt{N})$ as argued in class, and each $G'$ calls the oracle $Z_X$ once, so this is an $\mathcal{O}(\sqrt{N})$ quantum query algorithm for obtaining $|w\rangle$ with certainty.

### 5.2 The phase estimation algorithm

In class we showed that with probability greater than 1/2, given the ability to efficiently compute the order modulo $N$ of a positive integer relatively prime to $N$, one can efficiently find a factor of $N$. We then described a quantum algorithm $\mathcal{A}$ that with high probability[1] will, given a positive integer $N$ and an $x$ relatively prime to $N$, efficiently return positive integers $a$ and $b$ relatively prime to each other such that $a/b = k/r$, where $r$ is the order of $x$ modulo $N$ and $k$ is an integer that is (roughly) equiprobably chosen from $\{0, \ldots, r-1\}$. Repeating $\mathcal{A}$ $\mathcal{O}(\log N)$ times will yield a value of $k$ relatively prime to $r$ with probability

[1] With probability greater than $4/\pi^2$, a careful analysis reveals; see Preskill's notes Sec. 6.9.1 for details.

greater than 2/3, in which case $b = r$, the order of $x$ modulo $N$. (In fact, only a constant number of repetitions suffice—see Preskill's notes Sec. 6.9.1 for details.)

Alexei Kitaev discovered another, perhaps more intuitive, quantum algorithm for returning a fraction $k/r$ equiprobably over $k$ in $\{0, \ldots, r-1\}$ given relatively prime integers $x$ and $N$ such that the order of $x$ modulo $N$ is $r$. His algorithm relies on a general-purpose algorithm called the *phase estimation algorithm* described in Sec. 5.2 in your textbook by Nielsen and Chuang. Given the ability to perform $\Lambda(U^{2^j})$ for $j = 0, \ldots, m$ and an eigenstate $|u\rangle$ of $U$ with eigenvalue $e^{2\pi i\varphi}$, the phase estimation algorithm estimates the value of $\varphi$ to $m$ bits of precision.

The way that the phase estimation algorithm reproduces the action of $\mathcal{A}$ is as follows. Consider the unitary operator $U$ defined on $n = \lceil \log_2 N \rceil$ qubits as follows:

$$U|y\rangle = \begin{cases} |xy \bmod N\rangle & y < N \\ |y\rangle & N \le y \le 2^n. \end{cases} \tag{17}$$

The eigenvalues of $U$ are the $r$th roots of unity, $\lambda_k = e^{2\pi ik/r}$, because $U^r = I$. Moreover, the $n$-qubit state $|1\rangle$ is the uniform superposition over all eigenstates $|\lambda_k\rangle$, as shown in Sec. 5.3 in your textbook by Nielsen and Chuang. Hence, calling the phase estimation algorithm on $|1\rangle$ and $U$ will yield a fraction $k/r$, where $k$ is selected uniformly at random from $\{0, \ldots, r-1\}$.

In this problem, we *derive* the phase estimation algorithm as a "feedback filter," at least within a proscribed framework. Consider the "quantum feedback" circuit below.

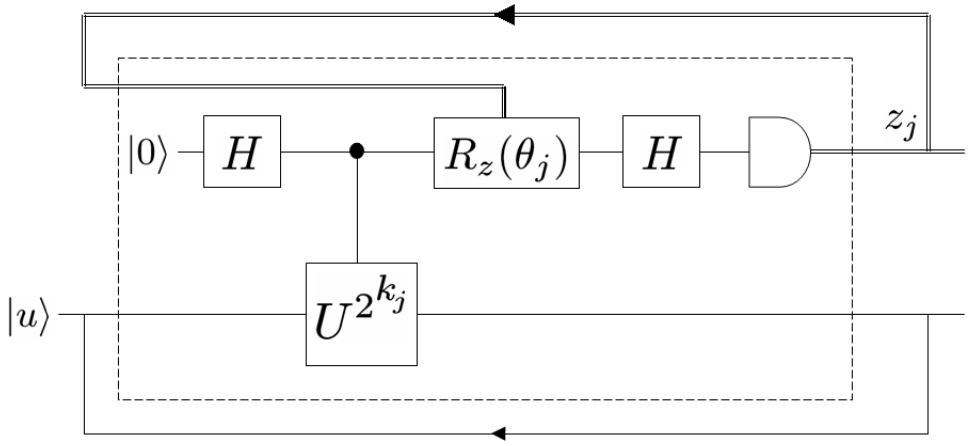


Figure 1: Feedback circuit for phase estimation.

The state $|u\rangle$ input to this circuit is an eigenstate of $U$ such that $U|u\rangle = e^{2\pi i\varphi}|u\rangle$ and $R_z(\theta)$ denotes the spin-1/2 rotation matrix $\exp(-i\pi\theta\sigma_z/2)$. After the $j$th pass through the loop, the classical output bit $z_j$ and quantum state $|u\rangle$ are fed back into the loop as indicated.

This circuit has two "control parameters," $\theta_j$ and $k_j$. $\theta_j$ is a function of both the round $j$ and all previous output bits $\{z_l\}_{l<j}$, while $k_j$ is solely a function of the round $j$.

The phase $0 \leq \varphi < 1$ is unknown but to make this problem simpler, let us suppose that it is guaranteed to have only $n$ bits of precision, *i.e.*, $\varphi = 0.\varphi_1\varphi_2 \ldots \varphi_n$ in (fractional) binary. This feedback circuit is said to be an "optimal exact phase estimator" if and only if the bits $z_1, \ldots, z_n$ determine $\varphi$ exactly. In this problem, you will show that this circuit is indeed an optimal exact phase estimator if $\theta_j$ and $k_j$ are chosen appropriately.

($a$) After passing through this circuit at round $j$, what are the probabilities of measuring $z_j = 0$ and of measuring $z_j = 1$ as functions of $k_j$ and $\theta_j$?

($b$) Show that it is possible to choose $k_1$ and $\theta_1$ so that $z_1 = \varphi_n$ with probability one.

($c$) Using the choices of $k_1$ and $\theta_1$ from part ($b$), show that it is possible to choose $k_2$ and $\theta_2(z_1)$ so that $z_2 = \varphi_{n-1}$.

($d$) In general, what choices of $k_j$ and $\theta_j(z_1, \ldots, z_{j-1})$ yield $z_j = \varphi_{n-j+1}$ with probability one? These choices are the "control law" that makes this circuit an optimal exact phase estimator.