MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Department of Physics, EECS, and Department of Applied Math

MIT 6.443J / 8.371J / 18.409 / MAS.865

Quantum Information Science

March 18, 2008

Problem Set #4

(due in class, 03-Apr-08)

Lecture Topics (3/18, 3/20, 3/25, 3/27, 4/1): quantum algorithms; entanglement

Recommended Reading: Nielsen and Chuang, Sections 5.4, 12.1 - 12.4, and Chapter 6

Problems:

P1: (**Quantum factoring as a feedback process**) Shor's quantum factoring algorithm was independently (re-)discovered by Alexei Kitaev, in Russia. Kitaev's formulation allows for an interesting observation of how quantum factoring can be viewed as a feedback process, involving quantum control and optimal estimation, as we explore in this problem.

Let N be a composite number we wish to factor, and choose some y coprime to N. Define the unitary transform U to be

$$U|m\rangle = |my \bmod N\rangle\,, \tag{1}$$

where the state lives in an N dimensional Hilbert space (for example, of $n = \lceil \log_2 N \rceil$ qubits).

(a) Show that the eigenstates of U are

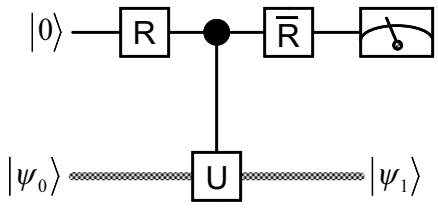
$$|\lambda_k\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i l \phi_k} |y^l \bmod N\rangle\,, \tag{2}$$

where $\phi_k = k/r$, and r is the order of y, i.e. the smallest integer such that $y^r \bmod N = 1$. Also show that

$$U|\lambda_k\rangle = e^{-2\pi i \phi_k} |\lambda_k\rangle\,. \tag{3}$$

It is a fact from number theory that once r is known, with probability greater than 50%, a factor of N can be found. Factoring N is thus equivalent to finding r. The calculation here indicates that finding r is equivalent to finding an eigenvalue of U. We consider next a circuit by which this may be accomplished.

(b) Consider this quantum circuit:



This is one step of a Kitaev factoring algorithm, in which the top wire carries an ancilla qubit, and the bottom (thick grey) wire carries the main n qubit state. Let the initial input state into the controlled-U gate be $|\psi_0\rangle = |\lambda_k\rangle$. The R gate acting on the ancilla qubit is the Hadamard transform

$$R = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} . \tag{4}$$

Following the initial state through the circuit, show that the ancilla is measured to be 0 with probability

$$p_0 = \cos^2(\pi\phi_k), , \tag{5}$$

and independent of the measurement result, the final state $|\psi_1\rangle = |\lambda_k\rangle$ for this example. Note that therefore, it may be reused.

The interesting observation is that after repeated trials, we are able to estimate p_0 and thus determine the eigenvalue ϕ_k. If we may repeat the procedure with powers of U, i.e., U^{2^j}, then we may estimate ϕ_k efficiently (in a number of trials polynomial in $\log N$).

(c) Unfortunately, the above scheme would not be very useful if we already knew enough to be able to generate an eigenstate at the outset to feed into the system! What happens if we do not start with an eigenstate, and instead have the input state

$$|\psi_0\rangle = |1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\lambda_k\rangle , \tag{6}$$

which is an equally weighted superposition of eigenstates?

Note that $|1\rangle$ is simple to generate. It is convenient to define the ancilla state

$$|\eta_k\rangle = \frac{1}{2} \left[(1 + e^{-2\pi i \phi_k})|0\rangle + (1 - e^{-2\pi i \phi_k})|1\rangle \right] . \tag{7}$$

Compute the output state after one trial, and show that it is given by

$$|\psi_1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\eta_k\rangle|\lambda_k\rangle . \tag{8}$$

(d) Compute the output state after t trials, $|\psi_t\rangle$, where the output of each trial is fed back as the input to the next iteration of the circuit.

(e) Each measurement of an ancilla qubit $|\eta_k\rangle$ gives either 0 or 1, and by symmetry, the order of results doesn't matter, so the only important quantity is the total number of zeros measured, n_0 out of the t trials. Let us try to understand what a-posteriori state results for a given n_0 by considering the joint probability distribution $p(k, n_0)$, where $n_1 = t - n_0$ is the number of one's

which resulted. This distribution is what one would obtain if a projective measurement were carried out on the $|\psi\rangle$ state in the $|\lambda_k\rangle$ basis. Give an expression for $p(k, n_0)$.

(f) The interesting thing is that to a very good approximation, $p(n_0) \approx 1/2$, and so the *conditional* probability for getting some k, given n_0, is

$$p(k|n_0) \approx \frac{2}{r}\binom{t}{n_0} \cos^{2n_0}\left[\frac{\pi k}{r}\right] \sin^{2n_1}\left[\frac{\pi k}{r}\right] . \tag{9}$$

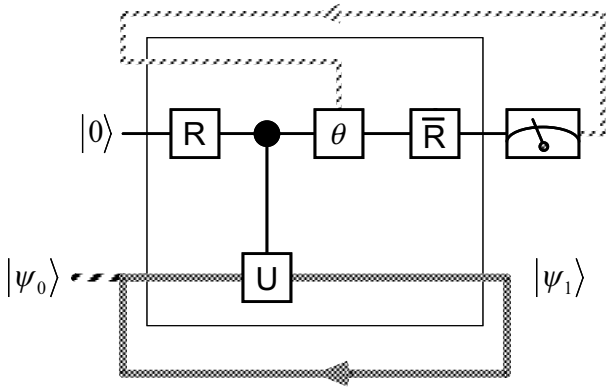
Verify this expression and plot the distribution; show that it has two peaks with widths which decrease as $\mathcal{O}(1/t)$.

This shows that with each successive increase of t, the state $|\psi_t\rangle$ increasingly converges into a superposition of two eigenstates of U, and moreover, knowledge of n_0 increasingly determines k.

(g) Helpful insight is gained by a numerical example. Try running this algorithm for $N = 143$, $y = 5$, and $r = 20$, and plot $p(k|n_0)$ for a sequence of values of t.

The critical quantity is the convergence rate of our knowledge of the eigenvalue.

(h) One of the inefficiencies of the scheme derived above is the fact that even after the system has converged into a perfect eigenstate, the measurement result from each iteration can still vary quite randomly. That is, once k has converged to a fixed value, we still obtain a zero with probability $\cos^2(\pi\phi_k)$, which can be significant. Ideally, we would like arrange the output distribution so as to maximize the mutual information between each measurement and the unknown eigenvalue ϕ_k. We can take a step in that direction by modifying the above quantum circuit to become:



Note that an additional component is added in the control path, a θ box, which implements the transform

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i\theta} \end{bmatrix} \tag{10}$$

on the control bit, where θ is a classically determined angle, provided by a classical control apparatus. Operation of this circuit is very similar to the previous scenario: an initial state $|\psi_0\rangle$ is prepared and fed into the lower loop. This state will continually circulate, and eventually converges into an eigenstate of the system.

The difference now is that depending on the accumulated sequence of measurement results, we can estimate the state of the system and change θ accordingly to bias future measurement outputs so that they have low entropy.

Analyze how this circuit works in detail, by following the state around one iteration of the loop, assuming it starts initially with an eigenstate input, $|0\rangle|\lambda_k\rangle$. Show that if we choose $\theta = \phi_k$ then $p_0 = 1$. This is good, because then a measurement of 1, being an unlikely event (if our estimator is correct), would give us a relatively large amount of information about the error $|\theta - \phi_k|$.

(i) Coming up with a good estimator model is nontrivial, especially since the system changes nondeterministically each time a measurement is performed. In particular, when feedback is performed, Eq.(9) is no longer a good estimate of the state, since the Hamiltonian now becomes a function of the record of prior measurement results!

Construct an algorithm for updating θ based on the measurement record obtained, using the idea that $\{f_0, f_1, \ldots\}$ is a model (series of functions of ϕ) of what we expect the system's conditional probability distribution for ϕ_k to look like, approximating $p(n_0) \approx 1/2$ (this is not very good at late times). Append new multiplicative terms to this function after each iteration, depending on the measurement results obtained.

Evaluate your algorithm, for example, using a trial run with parameters $N = 143$, $y = 5$, $r = 20$.

(j) [optional] The procedure suggested in the last step is somewhat unstable in practice, because the estimator for θ is very bad at early times. An improved solution would be to estimate θ based on a running average of ϕ, or from the frequency of occurance of 0. Ideally, you would want something like a Kalman filter. Try to derive an optimal estimation procedure for this feedback based quantum factoring algorithm, and compare your result with Shor's algorithm. What θ update rule would you need to be able to obtain the quantum Fourier transform circuit?

P2: (**Entanglement distillation**) Alice and Bob plan to use a quantum code to distill one pair of highly entangled qubits from some prior shared entanglement.

(a) Suppose Alice and Bob have nine entangled pairs, each in the state

$$(1 - 3\epsilon)|\psi_-\rangle\langle\psi_-| + \epsilon(|\psi_+\rangle\langle\psi_+| + |\phi_-\rangle\langle\phi_-| + |\phi_+\rangle\langle\phi_+|), \tag{11}$$

where $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ and $|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$. They measure the syndrome for the nine-qubit code and throw their quantum states away unless the syndromes both say "no error". If the syndromes both say no error, they decode to obtain a pair of entangled qubits. Compute (up to the ϵ^3 term) the resulting state of the qubits.

(b) Suppose that Alice and Bob both measure the same syndrome. Can they achieve an entangled qubit of the same accuracy as in (a)? How?

(c) Suppose they measure different syndromes. Suppose, for example, that Alice measures "no error" and Bob measures a "σ_X error". If Bob corrects his error and then they both decode, what state (up to ϵ^3) is their qubit in then?

P3: (**State Identification and the Pretty Good Measurement**) We will consider the general problem of distinguishing states of an ensemble.

(a) Suppose that we have states $\rho_1, \rho_2, \ldots, \rho_k$ which occur with probabilities $p_1, p_2, \ldots, p_k$. Show that if there is a positive Hermitian matrix τ such that $p_i\rho_i \leq \tau$ for all i, then Tr τ is an upper bound on the probability of success of a POVM measurement which tries to guess one the possibilities $1, \ldots, k$. Here $p_i\rho_i \leq \tau$ means that $\tau - p_i\rho_i \geq 0$, i.e., is positive.

The τ with minimum trace satisfying the conditions above actually gives the optimal probability of success. The proof of this uses semidefinite programming, and will thus not be covered in this class.

The *pretty good measurement* (PGM) is defined as follows. Given a set of density matrices ρ_i with associated probabilities p_i, let $M = \sum_i p_i \rho_i$. The PGM associated with this family of mixed states is $\{E_i\}$ where the measurement operators are $E_i = p_i M^{-1/2} \rho_i M^{-1/2}$. $M^{-1/2}$ is the unique positive operator such that $(M^{-1/2})^2 M$ is the projection operator onto the image of M.

(b) Suppose that a qubit is in state $|0\rangle + e^{2\pi i j/k}|1\rangle$ with probability $1/k$, $j = 0, \ldots, k-1$. What is the pretty good measurement for determining the state of this qubit. Show that it is optimal using part (a).

(c) Find a POVM measurement which does an equally good job of guessing the state of the above qubit, and has at most three different outcomes.

(d) Suppose you have a qubit that is in state $|0\rangle$ with probability 1/3 and in state $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ with probabilities 1/3 each. Use (a) to find an upper bound on the probability of success. Find a POVM which achieves this upper bound. What is the pretty good measurement in this case, and with what probability does it identify the correct outcome?

(e) Suppose you have a qubit prepared as above, except that it is in state $|0\rangle$ with probability 1/2 and in each of the other two states with probability 1/4. Use (a) to find an upper bound on the probability of success, and find a POVM which achieves this upper bound.

P4: (**Measures of pure state entanglement**) Entanglement is a property of a composite quantum system that cannot be changed by local operations and classical communications. How do we mathematically determine if a given state is entangled or not? And if a state is entangled, how entangled is it?

(a) Recall that by virtue of the Schmidt decomposition (book, page 109), a pure state $|\psi\rangle$ in the Hilbert space of systems A and B can be written as

$$|\psi\rangle = \sum_k \lambda_k |k_A\rangle |k_B\rangle \,, \tag{12}$$

where $|k_A\rangle$ and $|k_B\rangle$ are orthonormal states of systems A and B, respectively, and $\sum_k \lambda_k^2 = 1$. The *Schmidt number* is the number of nonzero λ_k. Prove that $|\psi\rangle$ is a product state, that is $|\psi\rangle = |\psi_A\rangle|\psi_B\rangle$, if and only if the Schmidt number of $|\psi\rangle$ is 1.

(b) Prove that the Schmidt number cannot be changed by local unitary transforms and classical communication. The Schmidt number is one measure of how entangled a state is.

(c) Give the Schmidt numbers for each of the following states:

$$|\phi_1\rangle = \frac{|00\rangle + |11\rangle + |22\rangle}{\sqrt{3}} \tag{13}$$

$$|\phi_2\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \tag{14}$$

$$|\phi_3\rangle = \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2} \tag{15}$$

$$|\phi_4\rangle = \frac{|00\rangle + |01\rangle + |11\rangle}{\sqrt{3}} \,. \tag{16}$$