Quantum algorithms (CO 781) Winter 2008

ASSIGNMENT 2 due Thursday 28 February (in class)

Problem 1 (*The hidden parabola problem revisited*).

Recall that in the hidden parabola problem, we are given a black box function $f_{\alpha,\beta} : \mathbb{F}_p^2 \to S$, where p is a prime, $\alpha \in \mathbb{F}_p^\times$ and $\beta \in \mathbb{F}_p$ are unknown parameters, and S is a finite set. For fixed α, β, the function $f_{\alpha,\beta}$ is promised to be constant on the parabola

$$P_{\alpha,\beta,\gamma} := \{(x, y) \in \mathbb{F}_p^2 : y = \alpha x^2 + \beta x + \gamma\}$$

for any particular $\gamma \in \mathbb{F}_p$, and distinct on parabolas corresponding to different values of γ. In this problem, you will find an efficient quantum algorithm to determine α, β by querying $f_{\alpha,\beta}$.

a. Write down the mixed quantum state obtained by querying $f_{\alpha,\beta}$ on a uniform superpositon over $\mathbb{F}_p \times \mathbb{F}_p$ and then discarding the function value.

b. Show that this state is invariant under additive translations of one of the two registers, and hence will be block diagonalized by the Fourier transform over $\mathbb{Z}_p$ on that register. Compute the resulting Fourier transformed state.

c. Suppose the register on which the Fourier transform was performed is measured, and consider the resulting post-measurement state. Show that this density matrix is rank one, and write down the pure quantum state to which it corresponds.

d. Write down the state obtained when the process described in parts a–c is performed twice. Collect the terms in the phase of this state proportional to the unknown parameters α, β, and show that these coefficients can be computed in ancilla registers.

e. For any fixed value of the two ancilla registers, compute the state of the other two registers. In particular, show that it is (proportional to) the uniform superposition over the set of solutions to a pair of quadratic equations in two variables.

f. Find the solutions of this system of quadratic equations. (You may want to use a computer algebra program to do the calculation.)

g. Explain how to efficiently erase the values in the registers containing the solution to the quadratic system.

h. Having implemented the erasure, perform the inverse Fourier transform over $\mathbb{Z}_p \times \mathbb{Z}_p$ on the ancilla registers, and show that a measurement of the resulting state gives the outcome α, β with probability $\Omega(1)$.

Problem 2 (*Classical random walk on glued trees*).

Consider a graph obtained by taking the union of two balanced binary trees of height n and joining their leaves by some cycle that alternates between the two sets of leaves. Suppose that a classical random walk (either continuous- or discrete-time, according to your preference) starts at the root of one of the trees. Prove that the probability of reaching the opposite root after any amount of time has passed is $2^{-\Omega(n)}$.

Problem 3 (*The Lie product formula*).

Let A and B be finite-dimensional Hermitian matrices, and let $\nu := \max\{\|A\|, \|B\|\}$.

a. Prove the *Lie product formula*, which states

$$\lim_{m\to\infty} (e^{-iAt/m} e^{-iBt/m})^m = e^{-i(A+B)t}.$$

b. Show that

$$\|(e^{-iAt/m} e^{-iBt/m})^m - e^{-i(A+B)t}\| \leq \epsilon$$

provided $m = \Omega(\nu^2 t^2/\epsilon)$.

c. How large should m be (as a function of ν, t, and ϵ) so that

$$\|(e^{-iAt/2m} e^{-iBt/m} e^{-iAt/2m})^m - e^{-i(A+B)t}\| \leq \epsilon?$$

Problem 4 (*The spectrum of a product of reflections*).

In lecture, we defined a discrete-time quantum walk on an n-vertex graph as the product of a reflection on $\mathbb{C}^n \otimes \mathbb{C}^n$ and the same reflection with the two systems interchanged. To analyze the walk, we computed the spectrum of this product of reflections. In this problem, you will generalize that calculation to the product of two arbitrary reflections.

Consider two subspaces

$$\mathcal{A} := \text{span}\{|\psi_1\rangle, \ldots, |\psi_a\rangle\} \qquad\qquad \mathcal{B} := \text{span}\{|\phi_1\rangle, \ldots, |\phi_b\rangle\}$$

of $\mathbb{C}^m$, where $\langle\psi_j|\psi_k\rangle = \delta_{jk}$ and $\langle\phi_j|\phi_k\rangle = \delta_{jk}$. Let

$$\Pi := \sum_{j=1}^{a} |\psi_j\rangle\langle\psi_j| \qquad\qquad \Sigma := \sum_{j=1}^{b} |\phi_j\rangle\langle\phi_j|$$

denote projections onto the two subspaces, let $R := 2\Pi - I_m$ and $S := 2\Sigma - I_m$ denote reflections about the subspaces, and let $U := RS$ denote their product. Finally, let D denote the $a \times b$ matrix with entries $D_{jk} = \langle\psi_j|\phi_k\rangle$. You will show how the spectrum of U can be obtained from the singular value decomposition of D.

a. Let $|\alpha\rangle$ and $|\beta\rangle$ denote left and right singular vectors of D, respectively, with the same singular value σ. The left singular vector $|\alpha\rangle \in \mathbb{C}^a$ can be mapped to a vector $A|\alpha\rangle \in \mathbb{C}^m$ by applying the isometry $A := \sum_{j=1}^{a} |\psi_j\rangle\langle j|$. Similarly, the right singular vector $|\beta\rangle \in \mathbb{C}^b$ can be mapped to a vector $B|\beta\rangle \in \mathbb{C}^m$ by the isometry $B := \sum_{j=1}^{b} |\phi_j\rangle\langle j|$. Show that the subspace $\text{span}\{A|\alpha\rangle, B|\beta\rangle\}$ is invariant under the action of U.

b. Diagonalize the action of U within this subspace to obtain one or two eigenvectors of U. When do you obtain one, and when do you obtain two?

c. Compute the eigenvalues of U corresponding to these eigenvectors.

d. How many eigenvectors of U are obtained by the procedure outlined above? What are the remaining eigenvectors of U and their corresponding eigenvalues?

Problem 5 (*Continuous- vs. discrete-time quantum walk*).

While the notions of continuous- and discrete-time quantum walk are conceptually related, the detailed behaviors of these two kinds of processes can differ. Nevertheless, in this problem you will establish a formal correspondence between them.

Szegedy's formulation of discrete-time quantum walk converts an arbitrary classical Markov chain, corresponding to an $n \times n$ stochastic matrix P, into a corresponding unitary operation on $\mathbb{C}^n \otimes \mathbb{C}^n$. The spectrum of this operation depends on the spectrum of the symmetric matrix $Q \circ Q^T$, where Q is the elementwise square root of P and $\circ$ denotes the Hadamard product. Consider the continuous-time quantum walk generated by a symmetric matrix H. If H can be factorized as $Q \circ Q^T$, where Q is the elementwise square root of a stochastic matrix P, then it defines a closely related discrete-time quantum walk via Szegedy's construction.

a. Let H be the adjacency matrix of a d-regular n-vertex graph. Show that H/d can be written as $Q \circ Q^T$, where Q is the elementwise square root of a stochastic matrix P.

b. More generally, let H be a symmetric matrix obtained by replacing the nonzero entries of the adjacency matrix of a connected graph by arbitrary positive numbers. Such a matrix is said to be *irreducible*. The *Perron-Frobenius Theorem* says that any irreducible symmetric matrix H has a principal eigenvector with strictly positive entries. Using this fact, show that $H/\|H\| = Q \circ Q^T$ for some Q that is the elementwise square root of a stochastic matrix P.

c. Compare the spectrum of $e^{iH/\|H\|}$ to the spectrum of the discrete-time quantum walk U corresponding to the classical Markov chain defined by P. In particular, suppose we define the *gap* of a unitary operator V as $\min\{|\arg \lambda| : \lambda \text{ is an eigenvalue of } V \text{ with } \lambda \neq 1\}$. Show that the gap of iU is at least the gap of $e^{iH/\|H\|}$. (In fact, you should be able to show that when the gaps are small, they are nearly identical).

d. *Challenge problem:* Now suppose that we obtain H by replacing the nonzero entries of the adjacency matrix of a connected bipartite graph by arbitrary nonzero complex numbers, subject only to the constraint that $H = H^\dagger$. Show that H can be written as some multiple of a matrix $Q \circ Q^\dagger$, where the rows of Q have unit length (under the ℓ_2 norm). Explain why this still allows us to define a discrete-time quantum walk corresponding to the continuous-time quantum walk generated by H, even though it does not necessarily let us define a corresponding classical Markov process.

   Alternatively, in light of Problem 4, show how to choose orthonormal sets of states $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ and $\{|\phi_1\rangle, \ldots, |\phi_n\rangle\}$ such that $H_{jk} = c\langle\psi_j|\phi_k\rangle$ for some constant c. (In this case you do not need to assume that graph of nonzero entries of H is bipartite.) Explain how this also lets us define a corresponding discrete-time quantum walk.