CS667/CO681/PH767 Quantum Information Processing (Fall 06)

Assignment 2

Due date: October 24, 2006

1. **Review of some basic properties of matrices.**

   (a) Prove that every $d \times d$ matrix M has at least one eigenvector. (An *eigenvector* is a state $|\psi\rangle \neq 0$ such that $M|\psi\rangle = \lambda|\psi\rangle$, where $\lambda \in \mathbb{C}$.)

   (b) Prove that, for all d, there exists a $d \times d$ matrix M that has only one eigenvector up to a multiplicative constant. (That is, for all d, there is some $d \times d$ matrix M for which there exists an eigenvector $|\psi\rangle$ such that *all* eigenvectors of M are scalar multiples of $|\psi\rangle$.)

   (c) Prove that, for every $d \times d$ matrix M, there exists a unitary operation U such that $M = U^\dagger T U$, where T is upper triangular. (Hint: try induction on d, and make use of the result in part (a) in the inductive step.)

   (d) A $d \times d$ matrix M is *normal* if $MM^\dagger = M^\dagger M$. Prove that M is normal if and only if, for some unitary operation U, $M = U^\dagger D U$, where D is diagonal. (Hint: you may use the result from part (c).)

   Note: intuitively, part (d) means that normal matrices are precisely those that have the property that there is an orthonormal basis in which they are diagonal. Normal matrices arise frequently in the setting of quantum information—for example unitary and Hermitian matrices are both special cases of normal matrices.

2. **Teleporting entanglement?**

   Recall the teleportation protocol that was covered in class. Alice and Bob start with the entanglement $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ (between them) and then Alice receives an arbitrary state $|\psi\rangle$. Alice performs a unitary transformation and then a measurement on the two qubits in her possession and then sends the resulting two classical bits to Bob, who can then reconstruct $|\psi\rangle$.

Now, suppose that, instead of having Alice receive $|\psi\rangle$, she receives the second qubit of some two-qubit state

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

that is *entangled* with a third party Carol. What happens if Alice follows the teleportation protocol with Bob to teleport her qubit (to Bob)? Is the result that Carol and Bob share the two-qubit state

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle?$$

Either prove that this is so or give an example of a state where this does not occur.

3. **Parity of three bits?**

   Recall the quantum algorithm for computing $f(0) \oplus f(1)$ with a single query to $f : \{0,1\} \to \{0,1\}$. This algorithm first constructs the state

   $$\tfrac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \tfrac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle$$

   with a single query to f and then performs a measurement on this state to exactly determine $f(0) \oplus f(1)$.

   Consider the possibility of generalizing this approach to computing $g(0) \oplus g(1) \oplus g(2)$ with a single query to $g : \{0,1,2\} \to \{0,1\}$. It is straightforward to construct the state

   $$\tfrac{1}{\sqrt{3}}(-1)^{g(0)}|0\rangle + \tfrac{1}{\sqrt{3}}(-1)^{g(1)}|1\rangle + \tfrac{1}{\sqrt{3}}(-1)^{g(2)}|2\rangle$$

   with a single query to g.

   Is there a measurement of this state that deduces the value of $g(0) \oplus g(1) \oplus g(2)$? Either give the measurement or explain why such a measurement is impossible.

4. **Slight variation of Simon's problem.** Consider the following variant of Simon's problem. The given function $f : \{0,1\}^n \to \{0,1\}^n$ has the the following property. There is a 2-dimensional subspace R of $\{0,1\}^n$ (viewed as a vector space in modulo 2 arithmetic) such that $f(x) = f(y)$ if and only if $x + y \in S \pmod 2$, and the goal is to find all the elements of R. Explain how to solve this problem by a quantum algorithm that makes only $O(n)$ queries to f and $O(n^3)$ auxiliary operations.

5. **Quantum one-way functions.** Intuitively, a *(bijective) one-way function* is a function that is easy to compute in the forward direction but difficult to invert. More precisely it is a family of functions $f_n : \{0,1\}^n \to \{0,1\}^n$ (one for each value of n) such that:

   - There exists a polynomial-time algorithm that, given $x \in \{0,1\}^n$, computes $f_n(x)$ in time polynomial with respect to n.
   - For all polynomial-time algorithms A, if $x \in \{0,1\}^n$ is randomly selected and $y \leftarrow f_n(x)$ then $\Pr[A(y) = x] = O(1/n^c)$, for all c (thus the success probability of the algorithm is asymptotically smaller than $1/n^c$ for all c).

   In classical complexity theory it is unknown whether or not one-way functions exist, but there are some candidate functions that are conjectured to be one-way, and they are employed in cryptographic protocols.

   Does it make sense for a family of functions $f_n : \{0,1\}^n \to \{0,1\}^n$ to be one-way with respect to *quantum* computers whose gates are unitary operations?

   Here is a sketch of a proposed proof that there are no one-way functions with respect to quantum computers. Suppose that there is a polynomial-size quantum circuit family $\mathcal{C}_n$ computing f_n in the sense that $\mathcal{C}_n|x\rangle = |f_n(x)\rangle$ for all $x \in \{0,1\}^n$. Since each gate in $\mathcal{C}_n$ is unitary, it has an inverse. Thus, reversing the order of all the gates and inverting them yields a circuit for f^{-1} whose size is the same as that of $\mathcal{C}_n$, and thus polynomial.

   Explain the error in this purported proof.