CO 781 Topics in Quantum Information **Instructor: Ashwin Nayak**
Homework #3 **Out: July 13, Due: August 3, 2004**

Note: Please remember to mention *all* your sources of help (colleague, research article, etc.).

Q. 1. Proof of security of QKD.
Verify the following steps in the Lo-Chau type entanglement purification protocol due to Shor and Preskill. (We follow the notation used in class.)

1. If in the testing (i.e., error rate estimation) part of the protocol, at most a fraction $\delta - \epsilon$ of errors are detected in the n test qubits (i.e., test EPR pairs), then the probability that the error rate in the *remaining* n EPR pairs is more than δ is exponentially small in n. Here, $0 < \epsilon < \delta$ is a small constant, and δ is the error correction threshold for the CSS code being used.

2. When Alice and Bob both measure error syndromes for bit and phase errors on their halves of n perfect shared EPR pairs, their state collapses to an entangled state over $Q_{x,z} \otimes Q_{x,z}$, where x, z are coset representatives that correspond to the observed error syndromes. This state is the same as the one obtained if Alice and Bob both encode their parts of m perfect shared EPR pairs using this code, where m is the number of information qubits in $Q_{x,z}$. Furthermore, if there are bit and phase errors (given by strings e_b, e_p, respectively) in the n EPR pairs, then the collapsed state is a similar entangled state over $Q_{x,z} \otimes Q_{x \oplus e_b, z \oplus e_p}$.

Q. 2. Properties of random walks.
Let P be a symmetric stochastic matrix corresponding to a Markov Chain $\mathcal{M}$. Using only basic facts from linear algebra (such as properties of real symmetric matrices), prove the following about P:

1. All the eigenvalues of P lie in the interval $[-1, 1]$.

2. If $\mathcal{M}$ is irreducible, then $\lambda_2(P)$, the second largest eigenvalue of P, is strictly smaller than 1.

3. If -1 is an eigenvalue of P, then the graph underlying $\mathcal{M}$ has a bipartite component. In other words, if $\mathcal{M}$ is aperiodic, the smallest eigenvalue is strictly larger than -1.

Therefore conclude that for an irreducible, aperiodic Markov Chain $\mathcal{M}$ defined by a symmetric stochastic matrix P, there is a unique stationary distribution: $P^t s$ tends to the uniform distribution on the states as t tends to infinity, for every initial distribution s.

Q. 3. Quantum walk algorithms.
In the *collision problem*, we are given a function $f : [n] \mapsto [n]$ as an oracle. We are promised that f is either a permutation or is 2-to-1 (i.e., for every $j \in [n]$, $|f^{-1}(j)|$ is either 0 or 2). Describe and analyse a quantum walk based algorithm to distinguish the two cases. Minimize the number of oracle queries that your algorithm makes, and calculate the time and space complexity.

Q. 4. Query lower bounds.
Consider a Boolean function $f : \{0,1\}^n \mapsto \{0,1\}$ and the sets $A_0 = f^{-1}(0), A_1 = f^{-1}(1)$. Suppose the string $X = X_1, X_2, \ldots, X_n$ chosen uniformly at random from the set A_i (for any $i \in \{0,1\}$) is k-wise independent. In other words, suppose that any set of k bits of X are uniformly distributed over $\{0,1\}^k$. Using any method of your choice, prove a lower bound of $\lceil k/2 \rceil$ for the bounded-error quantum query complexity of f. Conclude that the query complexity of the parity function is $\lceil \frac{n}{2} \rceil$.