CO 781 Topics in Quantum Information **Instructor: Ashwin Nayak**
Homework #1 **Out: May 11, Due: May 25, 2004**

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

Q. 1: 3-into-1 random access code. Show that there is an encoding of three bits into a single qubit, such that you can make an appropriate measurement to get any single bit of your choice with probability at least some constant $p > 1/2$.

Q. 2: Optimality of quantum fingerprints. Show that we need $n \in \Omega(\log m)$ qubits for fingerprinting, i.e., for constructing 2^m states $|\phi_x\rangle \in \mathbb{C}^n$, $x \in \{0,1\}^m$, such that $|\langle\phi_x|\phi_y\rangle|$ is at most a constant $\epsilon < 1$, for all $x \neq y$.

Q. 3: Communication with shared entanglement. Suppose Alice and Bob share k EPR-pairs, i.e., the state

$$\frac{1}{2^{k/2}} \sum_{a \in \{0,1\}^k} |a\rangle|a\rangle$$

where the first k qubits are with Alice, and the rest with Bob. Suppose that Alice now performs a unitary transformation on her part of the state and some ancilla, and sends m qubits to Bob.

(a) Prove that Bob's state may be represented as a mixture $\{p_i, |\phi_i\rangle\}$, where $p_i \leq 2^m/2^k$, and the states $|\phi_i\rangle$ are all orthonormal.

(b) Conclude that if Alice wishes to communicate a uniformly random n-bit string x to Bob using an m-qubit message, then their probability of success (Bob decoding x correctly from the message and his share of the EPR pairs) is at most $2^{2m}/2^n$.

Note that the bound above is independent of the number of EPR pairs originally shared by the two parties.

Q. 4: Communication complexity of Inner Product.

(a) Apply Razborov's method to show that the bounded-error quantum communication complexity of the Inner Product function

$$f(x,y) \quad = \quad \bigoplus_{i=1}^{n} (x_i \wedge y_i)$$

is $\Omega(n)$. Prove any polynomial degree lower bound you use. (Please do not repeat proofs we saw in class. Indicate how you may appeal to them to show the bound.)

(b) Explain how the above lower bound implies that the query complexity of the Parity function $x \in \{0,1\}^n \mapsto \bigoplus_{i=1}^n x_i$ is $\Omega(n/\log n)$.