CO 781 Topics in Quantum Information **Instructor: Ashwin Nayak**
Homework #2 **Out: June 8, Due: June 22, 2004**

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

Q. 1: Relationship between trace distance and fidelity.
Fuchs and Caves proved that there is a complete von Neumann measurement—i.e., an orthonormal basis—such that the fidelity between two mixed states is equal to the fidelity between the two classical mixtures (on outcomes) that is obtained by measuring the states in that basis. Moreover, the fidelity of these classical mixtures is the *minimum* fidelity over all possible measurements of the resulting distributions on outcomes.

Using this fact (or, by any other method you prefer), show that for single qubit states ρ_0, ρ_1:

$$1 - F(\rho_0, \rho_1) \quad \leq \quad \frac{1}{2} \| \rho_0 - \rho_1 \|_{\mathrm{tr}} \quad \leq \quad \sqrt{1 - F(\rho_0, \rho_1)} \, ,$$

where $F(\rho_0, \rho_1) = \left\| \sqrt{\rho_0}\sqrt{\rho_1} \right\|_{\mathrm{tr}}^2$ is the fidelity of the two states. [Compare this to the relationship between trace distance and fidelity we saw in class.]

Q. 2: Strong coin flipping.
Suppose that in the Aharonov, Ta-Shma, Vazirani, and Yao schema for strong coin flipping, one qu*bit* is sent in the first (commitment) message. (The protocol we saw in class uses a qu*trit*.) Show that the smallest possible cheating probability achievable in such a protocol is half the Golden ratio:

$$\frac{1}{4}\left(1 + \sqrt{5}\right) \quad = \quad 0.809\ldots .$$

In other words:

1. Devise and analyse an ATVY-type protocol for strong coin-flipping which uses a single qubit in the first message and has the above maximum cheating probability, and
2. Show that in *any* protocol following the ATVY schema, and using a single qubit in the first message, at least one party can cheat with the above probability.

(So, there is a definite advantage in using qutrit states in the ATVY schema.)

Q. 3: Quantum error-correcting codes.
In this problem, we will construct a quantum error-correcting code over a p-ary alphabet based on the classical Reed-Solomon code. The code will be a subspace of $\mathcal{H}^{\otimes n}$, where $\mathcal{H} = \mathbb{C}^p$ and $p > n$ is a prime.

Let ω be a primitive pth root of unity.

1. Define two operators B, P on $\mathcal{H}$ as follows:

$$\begin{aligned} B &: |a\rangle \mapsto |a+1 \pmod p\rangle \qquad (\text{“Bit flip” error}) \\ P &: |a\rangle \mapsto \omega^a |a\rangle \qquad (\text{“Phase flip” error}) \end{aligned}$$

   Prove that the ring generated by B and P is the entire space of linear operators on $\mathcal{H}$.

   What finite set of unitary error operators for quantum error correction does this property suggest?

2. Given the values of a univariate polynomial $f : \mathbb{Z}_p \mapsto \mathbb{Z}_p$ of degree at most r at $n \geq r+1$ non-zero points, its value at 0 is uniquely determined by the Lagrange interpolation formula:

$$f(0) \quad = \quad \sum_i f(i) \prod_{j \neq i} \frac{0-j}{i-j}.$$

   Let $c_i = \prod_{j \neq i} \frac{-j}{i-j}$ be the corresponding interpolation coefficients.

   Define a quantum transform U_c on $\mathcal{H}^{\otimes n}$ as follows: $U_c = \otimes_{i=1}^n F(c_i)$, where $F(c_i)$ is the quantum Fourier transform on $\mathcal{H}$ defined with respect to ω^{c_i}:

$$F(c_i) \quad = \quad \frac{1}{\sqrt{p}} \sum_{k,x \in \mathbb{Z}_p} \omega^{c_i k x} |k\rangle\langle x|$$

   Consider the linear classical code $C \subset \mathbb{Z}_p^n$ consisting of words $(f(1), f(2), \ldots, f(n))$, where $f : \mathbb{Z}_p \mapsto \mathbb{Z}_p$ is a polynomial of degree at most r that evaluates to 0 at 0 (i.e., $f(0) = 0$). Prove that

$$U(c)|C\rangle \quad = \quad |C^\perp\rangle,$$

   where $C^\perp = \{(g(1), g(2), \ldots, g(n)) : g \text{ is a polynomial of degree at most } n-r-1\}$ (also a Reed-Solomon code).

   How does this generalize to a coset C_a of C corresponding to translation by a constant a (which is a degree zero polynomial)?

   The states $|C_a\rangle$ form the basis for the quantum code.

3. Finally, we consider duality of bit and phase flips. How does the property of C_a above generalize to a codeword corrupted by a phase flip P^j in the ith location?

Q. 4: Privacy amplification.

In this problem, we will learn a piece of an alternative proof of security due to Ben-Or for the BB84 protocol. The piece concerns *privacy amplification*, and is captured by the following situation.

Alice and Bob share a random n-bit string x, and Eve has m qubits of information about x. In other words, the joint state of Alice, Bob and Eve may be written as

$$\sum_x \frac{1}{2^n} |x\rangle\langle x|_A \otimes |x\rangle\langle x|_B \otimes \rho_x.$$

To extract one bit k of secret key, Alice now picks a random n-bit string y, and sends it over an authenticated public classical channel to Bob. They both compute k as the inner product modulo 2 of x and y.

Argue that if $m = o(n)$, then Eve cannot predict the bit k with probability more than $\frac{1}{2} + o(1)$. Thus argue that regardless of the measurement Eve makes after seeing the string y, the conditional distribution of k given her measurement outcome is at most $o(1)$ away from uniform in ℓ_1 distance.