Homework 2

Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

1. Suppose Alice does a measurement $\{M_k : \mathcal{H}_A \to \mathcal{H}'_A\}$ on her register A, and Bob does a measurement $\left\{\tilde{M}_\ell : \mathcal{H}_B \to \mathcal{H}'_B\right\}$ on his register B. What is the global measurement that is being done on the whole system $A \bigotimes B$? Similarly, assume Alice does a POVM $\{E_k\}$ on A and Bob a POVM $\{E'_\ell\}$ on B, what is the POVM being done on the system $A \bigotimes B$?

2. A measurement M distinguishes ρ_1 from ρ_2 with zero error, if it has three possible answers $1, 2, quit$, and whenever it answers a non-quit value it is correct. We say M succeeds with probability p if for every input from $\{\rho_1, \rho_2\}$ it answers the correct value with probability at least p.

   - Find the bast value p with which a zero-error measurement can distinguish $|0\rangle\langle 0|$ from $|+\rangle\langle +|$.
   - find a three-dimensional measurement that achieves this value.

3. Show that a density matrix has rank 1 iff it represents a pure-state.

4. Compute the matrices A^0,A^1,B^0 and B^1 defined in class during the analysis of the quantum algorithm for the CHSH game. Compute the tensors $A^0 \bigotimes B^0$, $A^0 \bigotimes B^1$ $A^1, \bigotimes B^0$ and $A^1 \bigotimes B^1$ and show that no matter what questions $(s,t) \in \{0,1\}^2$ are asked, the winning probability of Alice and Bob is $cos^2(\pi/8)$.

5. (Magic Square game) Consider the following game:

   - Alice is given a question $i \in \{1, \ldots, 6\}$ and has to answer with a vector $(A_1, A_2, A_3) \in \{0,1\}^3$. Bob is given a question $j \in \{1, \ldots, 9\}$ and has to answer with a bit $B \in \{0,1\}$.
   - The referee asks correlated questions. It first picks $j \in \{1, \ldots, 9\}$ uniformly at random. It represents j as $j = 3a + b$ with $a \in \{0,1,2\}$, $b \in \{1,2,3\}$. Then, it picks $r \in \{1,2\}$ uniformly at random. If $r = 1$ the referee sets $i = a + 1$ and $k = b$. If $r = 2$ the referee sets $i = 3 + b$ and $k = a + 1$. The referee sends Alice the question i and Bob the question j and gets answers $A = (A_1, A_2, A_3) \in \{0,1\}^3$ from Alice and $B \in \{0,1\}$ from Bob.

   The players win the game iff:

   - The parity of the three bits in the answer of Alice is even when $i \in \{1,2,3\}$ and odd when $i \in \{4,5,6\}$, and,
   - $B = A_k$.

   what is the maximal winning strategy for a classical (deterministic or probabilistic) strategy. Find such a strategy.

6. (Classical coin flipping). Alice and Bob don't trust each other and want to toss a fair coin over the telephone. Alice and Bob are probabilistic TMs. A protocol is a multi-round, private-coin interactive protocol. I.e., for any given history it specifies the player who plays next and the message that player should send (the message may depend on the player's private random coins). It also specifies when the protocol terminates, and the value of the game (i.e., who won) when that happens.

   Show that in every such protocol there is a player that can cheat and force a win (with probability 1).