Homework 7
Due 2006/5/28

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

1. Give an alternative approach to the Marriott-Watrous witness-preserving QMA amplification based on eigenvalue estimation of $\Pi_1 + \Pi_2$. Hint: use Trotter's formula; also, make sure that the witness is still an m qubit state!

2. It is known that QMA is contained in PSPACE (and in fact in somewhat smaller classes). Let us show this using witness-preserving amplification.

   (a) Given any QMA verifier V_x, we defined a $2^m \times 2^m$ Hermitian matrix Q_x that gives the acceptance probability of any witness $|\psi\rangle$ as $\langle\psi|Q_x|\psi\rangle$. Show that we can compute any given entry of this matrix in polynomial space. Deduce that we can also compute its trace in polynomial space.

   (b) Prove that QMA $\subseteq$ PSPACE.

3. We have a quantum circuit (see Figure 1) whose input is an arbitrary quantum state $|\psi\rangle$ on m qubits and some ancilla qubits $|0^k\rangle$ on k qubits. Its output is a 'success' qubit and an output register $|\phi\rangle$ (on $m + k - 1$ qubits). The computation is *successful* if, when measuring the success qubit in the computational basis, the result is $|1\rangle$. The *output* of the circuit is the state $|\phi\rangle$, conditioned on success.

   (a) Show that we can *boost* the success probability of the circuit on *classical* inputs: there exists another circuit that given any classical input state $|\psi\rangle$ whose acceptance probability (in the original circuit) is, say, $p > 0.1$, gives the same output with success probability (exponentially) close to 1.

   (b) Now assume, in addition, that for *any* input $|\psi\rangle$, the success probability of the circuit is some *fixed* $0.1 < p < 1$. Show, as before, that the success probability can be boosted (for any input, not just classical states).

   (c) Try to explain why boosting is impossible if the success probability is not fixed over all $|\psi\rangle$.

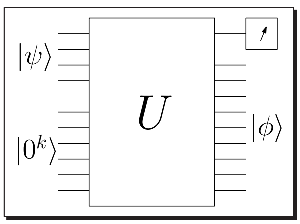

Figure 1: Boosting

4. Our goal is to show that Group Membership (GM) is in NP relative to any group oracle. Recall that we are given group elements $h, g_1, \ldots, g_k \in G$ and our goal is to find a way to verify that $h \in H := \langle g_1, \ldots, g_k\rangle$ (in time polynomial in $\log|G|$).

(a) Show that for any $A \subseteq G$, if $b \notin A^{-1}A$ (i.e., b cannot be written as $a_1^{-1}a_2$ for some two elements in A), then $|A \cup Ab| = 2|A|$.

(b) Show that for any strict subset $A \subsetneq H$, there exists an i and an element $a \in A$ such that $ag_i \notin A$.

(c) For a sequence of elements $a_1, \ldots, a_r$ define the 'cube' generated by them as

$$C(a_1, \ldots, a_r) := \{a_1^{b_1} \cdots a_r^{b_r} \mid b_1, \ldots, b_r \in \{0, 1\}\}.$$

Use this to show that there exists a witness (verifiable in polynomial time) to the property $h \in H$.