Q. Inf. Science II (6.443/8.371/18.436) — Spring 2018

Assignment 4

Due: **Friday**, *April 20, 2018 at* ***5pm***

Problem Set 4b - written part

Maybe hidden parabola, part a

1. **Group Non-membership in QMA** Suppose we are given a "black-box group" G. This means that the elements are encoded by unique n-bit strings (say g is represented by $E(g)$) and group operations are performed by an oracle which can perform multiplication, inverses and can check if an element is equal to the identity. That is, given $E(g), E(h)$ the oracle can output $E(gh)$ or $E(g^{-1})$ or can tell us if $g = e$ where e is the identity element. (For the rest of the this problem, we use g and $E(g)$ interchangeably.) Given an n-bit string, the oracle can also tell us whether it is a valid group element or not.

   The input to the group non-membership problem is a subgroup $H \subseteq G$ (specified by a list of generators) and an element $x \in G$. The answer is "yes" if $x \notin H$ and "no" if $x \in H$. (The group membership problem can be shown to be in NP. This is easy but not trivial [L. Babai, E. Szemerédi: On the complexity of matrix group problems I, in: Proc. 25th IEEE FOCS, FL, 1984, pp. 229-240.].) Group nonmembership, on the other hand, is not known to be in NP.

   In this problem you will show that the group non-membership problem is contained in QMA. The complexity class QMA is similar to NP but uses a quantum proof and quantum poly-time verifier. Formally a language L is in QMA if there is a poly-time quantum algorithm A that takes as input both the string x (whose membership in L we want to decide) and a "witness" state $|\psi\rangle$ of poly($|x|$) qubits. This algorithm should have the property that:

   - if $x \in L$ there exists $|\psi\rangle$ such that A accepts on input $x, |\psi\rangle$ with probability $\geq 2/3$;
   - if $x \notin L$ then for any $|\psi\rangle$ the probability that A accepts on input $x, |\psi\rangle$ is $\leq 1/3$.

   We sometimes call the verifier "Arthur" and the prover (who supplies $|\psi\rangle$) "Merlin." The name QMA stands for "Quantum Merlin-Arthur."

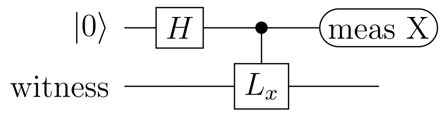
   (a) Consider the following protocol for solving group nonmembership in QMA. The witness is (ideally)

   $$|H\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle \,. \tag{1}$$

   Define the left-multiplication unitary to be

   $$L_x := \sum_{y \in G} |xy\rangle \langle y| \,. \tag{2}$$

Arthur's verification circuit is

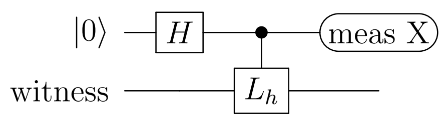


(3)

Here "witness" could be $|H\rangle$ but below we will consider the possibility that Merlin sends some other state. Show that if Merlin sends the state $|H\rangle$ then this protocol has the following behavior: if $x \in H$ then it always outputs 0 and if $x \notin H$ then it has 1/2 probability of outputting 1. (This is not quite the 2/3 vs. 1/3 behavior in the definition of QMA, but repeating it once will be enough amplification so that it satisfies the usual definition.)

(b) Unfortunately Merlin may not always be polite enough to send Arthur the state $|H\rangle$. Give an example of how Merlin can fool the protocol in (3) by choosing some other witness state.

(c) We can rescue this protocol by adding a step to verify that the witness is indeed the state $|H\rangle$ or at least something functionally equivalent. The protocol is



(4)

where h is a uniformly random element of H. (This can be generated in poly(n) time according to [L. Babai. "Local expansion of vertex-transitive graphs and random generation in finite groups." Theory of Computing, pp 164-147, 1991]. Technically h is only nearly uniformly random but we can ignore this here.) If the output is 0 then we continue with the protocol and if the output is 1 then we reject. Show that the probability of accepting a witness $|\psi\rangle$ here is equal to $\langle\psi| M |\psi\rangle$, where

$$M = \frac{I - \mathbb{E}_{h\in H}[L_h]}{2}, \tag{5}$$

and $\mathbb{E}$ means the expectation.

(d) Show that the eigenvalues of M are 1/2 and 1. By repeating $\log(1/\epsilon)$ times we can obtain a measurement with eigenvalues ϵ and 1. Thus we can assume that Merlin sends a state which is a 1-eigenvector of M. Alas, there are more of these than just $|H\rangle$. However, show that any 1-eigenvector of M (i.e. satisfying $M|\psi\rangle = |\psi\rangle$) will work as a witness in the protocol in (3).

(e) Now suppose that we have a black-box group but with an encoding that is not necessarily unique; i.e. there may be many n-bit strings that correspond to the same group element. Will this protocol still work or will something go wrong?