Problem Set #2

CMSC 858L
Instructor: Daniel Gottesman

Due on Gradescope Mar. 2, 2023, noon

The late deadline to turn the problem set in without penalty is Mar. 5, 2023, noon.

Problem #1. Bounding a restricted version of QMA(50 pts.)

Let $\mathrm{QMA}_{\log}$ be the class of languages in QMA for which the witness (for a yes instance, or for prospective witnesses for a no instance) is always of logarithmic size $O(\log |x|)$ qubits rather than polynomial size. In this problem, we will prove that $\mathrm{QMA}_{\log} \subseteq \mathrm{PSPACE}$.

For the purposes of this problem, fix a language in $\mathrm{QMA}_{\log}$ and the checking circuit for the language. You can assume that all amplitudes used in the quantum gates of that checking circuit are numbers of fixed precision independent of problem size.

a) (10 pts.) Suppose we write a potential witness $|\psi_x\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle$, where the witness lives in a Hilbert space of dimension $D = O(\mathrm{poly}(|x|))$. Show that the acceptance probability of the witness using a polynomial-size quantum checking circuit can be written as a polynomial in the α_i's and that the polynomial itself can be computed using polynomial space as a function of $|x|$.

b) (10 pts.) Show that if $|\alpha_i - \alpha_i'| < \delta$ for all i, where $|\psi_x'\rangle = \sum \alpha_i' |i\rangle$, then the acceptance probability of $|\psi_x'\rangle$ is within $O(\mathrm{poly}(D, \delta))$ of the acceptance probability of $|\psi_x\rangle = \sum \alpha_i |i\rangle$.

c) (10 pts.) Let us call a quantum state $|\psi\rangle = \sum_j \beta_j |j\rangle$ *δ-discretized* if each β_i is equal to δ times a Gaussian integer (i.e., of the form $a + bi$, where a and b are integers and $i = \sqrt{-1}$). Show that for a language in $\mathrm{QMA}_{\log}$, there exists a function $\delta(|x|) = \Omega(\mathrm{poly}(1/|x|))$ such that, for any instance x, the following hold:

- If x is a "yes" instance, then there exists a $\delta(|x|)$-discretized witness $|\psi_x'\rangle$ on $O(\log |x|)$ qubits) that is accepted with probability at least 5/9
- If x is a "no" instance, then any $\delta(|x|)$-discretized witness $|\psi_x'\rangle$ on $O(\log |x|)$ qubits will be rejected with probability at least 5/9.

d) (10 pts.) Consider the polynomial inequality $f(y_0, \ldots, y_{D_1}) \geq 0$, where f is a polynomial and the y_i's are integers with $|y_i| \leq N$ (here $|\cdot|$ means absolute value). Let L be the language which consists of all f such that the polynomial inequality is satisfied for some value of $(y_0, \ldots, y_{D_1})$. Show that L can be decided in a space $O(\mathrm{poly}(D, \log N))$.

e) (10 pts.) Prove $\mathrm{QMA}_{\log} \subseteq \mathrm{PSPACE}$.

Problem #2. Semi-local simulation of the Clifford group (50 pts.)

A stabilizer state is any state that can be created by applying a Clifford group circuit to the all 0s state $|00\ldots0\rangle$. Imagine we have a stabilizer state where the qubits are in spatially separated locations, possibly with multiple qubits in each location. A *local* Clifford circuit is one for which each layer is a tensor product of Clifford group gates on the different locations, and in particular, there are no gates that span multiple locations. At the end of the circuit, all qubits are measured in the standard basis.

A *local* classical simulation is one where after an initial set-up phase that depends on the state (but not the circuit) and may involve communication, all classical computations (which now depend on the circuit) are themselves local, involving only data and computation at each location separately. To be clear, here is the structure of a local classical simulation:

1. We are given a description of a stabilizer state $|\psi\rangle$ (provided by giving its stabilizer) with a specified split between multiple sites. Using classical communication and storage, we set up variables localized to each site.

2. We are given the description of a local Clifford circuit. Each site is only informed of the part of the Clifford circuit at its own location.

3. We now must perform local classical computations at each site to perform the simulation.

4. Each site outputs one or more bits.

In all cases in this problem, the goal is to perform an exact *weak* simulation, i.e. to output bit strings with exactly the same probability distribution as the corresponding quantum circuit.

a) (10 pts.) Suppose the initial state $|\psi\rangle$ is an n-qubit stabilizer state which is a tensor product between 2 sites. Show that there is an efficient local classical simulation of any local Clifford circuit acting on $|\psi\rangle$.

b) (10 pts.) Suppose the initial state is $|\psi\rangle = |00\rangle + |11\rangle$, which has stabilizer generated by $M_1 = X \otimes X$ and $M_2 = Z \otimes Z$, with the two qubits split between separate sites. Consider local Clifford circuits consisting of a tensor product of two single-qubit Clifford group gates, followed by standard basis measurement. Find a local classical simulation of this family of circuits.

c) (10 pts.) Now suppose the initial state is the three-qubit state $|000\rangle + |111\rangle$ (stabilizer generated by $M_1 = X \otimes X \otimes X$, $M_2 = Z \otimes Z \otimes I$, $M_3 = I \otimes Z \otimes Z$) split between 3 sites. Show that if each site *does* learn the full Clifford circuit, including gates applied to other sites, that there is an otherwise local simulation of the circuit.

d) (10 pts.) Again consider the state $|000\rangle + |111\rangle$ split between 3 sites. This state displays non-locality under local Clifford circuits and measurements, and thus there is no fully local classical simulation (efficient or inefficient) where the sites do not know the Clifford group gates on the other sites. Find a classical simulation in which one site is allowed to broadcast one or two classical bits of information to the other sites, but the simulation is in other respects local. (It is possible to do this with 1 bit, in fact, but 2 is easier.)

e) (10 pts.) Suppose you are given an arbitrary stabilizer state split between 2 sites A and B each with n qubits and the local Clifford circuits on sites A and B use T_A and T_B Clifford group gates, respectively. Find a classical simulation with $O(\mathrm{poly}(n, T_A, T_B))$ which is local except for a transmission of $O(n^2)$ classical bits from A to B, independent of T_A and T_B. (Note that no communication from B to A is allowed.)