Quantum Proofs, Semester A 2024

Homework # 1 **due: 5pm, December 28th, 2024**

Ground rules:

Homework is due through Moodle. If you are having issues with this, email the instructor (thomas.vidick@weizmann.ac.il) or drop your work in my mailbox at the top of the central stairs in Ziskind. Solutions can be latexed or handwritten. In the latter case, please make sure that your handwriting is legible. Special care should be taken in writing up a precise solution. If I am not able to follow the logic in your argument, if there is a small gap or an uncovered case, you will lose points.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded.

The first problem can be attempted immediately. Part (b) has no subtlety, but determining A requires writing the the acceptance probability of a QMA verifier in the appropriate manner — as a maximum eigenvalue problem, as discussed in class. The second problem can also be attempted immediately, granted that one accepts the equality $\mathsf{QMA} = \mathsf{QMA}_{c,s}$ *for any* $2^{-\mathrm{poly}} \leq s < c \leq 1 - 2^{-\mathrm{poly}}$ *such that* $c - s > 1/\mathrm{poly}$*, as claimed in class and which we will prove on 19/12. The third problem requires the lecture from 19/12.*

Any changes since the first posting will be marked in blue.

Problems:

1. (3 points) **The Trace Power Method and the Complexity of** QMA

   (a) Let A be a $D \times D$ positive semidefinite matrix. Show that the following inequality holds:

   $$\lambda_{max}^t \leq \mathrm{Tr}(A^t) \leq D\lambda_{max}^t$$

   where λ_{max} is the largest eigenvalue of A.

   (b) Let C be a QMA verifier circuit with q input qubits and one output qubit. Let $n = |C|$ be the size of C. Determine an operator A, depending on C, and an integer t such that computing $\mathrm{Tr}(A^t)$ would allow you to determine whether C satisfies the YES case (there is a quantum proof accepted by C with probability at least $\frac{2}{3}$) or the NO case (no quantum proof is accepted by C with probability larger than $\frac{1}{3}$).

(c) Use your answer from part (b) to argue that there is a polynomial-*space* algorithm that can decide any language in QMA, i.e. show the inclusion QMA $\subseteq$ PSPACE. Describe the algorithm in high-level language and explain carefully why it only requires a polynomial (in its input length, i.e. $|C|$) amount of space.

2. (4 points) **Non-identity check**
Consider the following promise problem (a, b)-*non-identity check* (NIC for short). The input is a description of a quantum unitary circuit U on m qubits. In the YES case, it is promised that there is an m-qubit state $|\psi\rangle$ such that $\||\psi\rangle - U|\psi\rangle\| \geq a$. In the NO case, it is promised that for all m-qubit states $|\phi\rangle$, $\||\phi\rangle - U|\phi\rangle\| \leq b$.

   (a) By giving an explicit verification procedure, show that for any $0 \leq b < a \leq \sqrt{2}$ such that $b - a > 1/\text{poly}(n)$, the problem (a, b)-NIC is in QMA.

   (b) Show that there are $0 \leq b < a \leq \sqrt{2}$ such that $b - a > 1/\text{poly}(n)$ for which the problem (a, b)-NIC is QMA-hard. *[Hint: given a unitary QMA verification circuit V, define a unitary U that, informally, executes V, saves the "answer", and "resets" the workspace used by V.]*

3. (3 points) **Small witnesses**
Consider a promise problem $L = (L_y, L_n) \in$ QMA and a QMA verification circuit $C = C_x$ for L that operates on quantum proofs on $q = q(n)$ qubits (where $n = |x|$).

   (a) Show (using a result from class) that there is a QMA verification circuit for L with proof states of $q(n)$ qubits, completeness $c \geq 1 - \delta$ and soundness $s \leq \delta$ where $\delta = \frac{1}{3}2^{-q(n)}$.

   (b) Suppose we execute the verification circuit from (a) on a uniformly random $q(n)$-qubit computational basis state. Show that if $x \in L_y$ then the acceptance probability is at least $\frac{2}{3}2^{-q(n)}$, while if $x \in L_n$ then it is at most $\frac{1}{3}2^{-q(n)}$.

   (c) Use (b) to show that QMA with proof states restricted to $q(n) = O(\log n)$ qubits *equals* BQP.

4. *(Optional problem, not for credit)* **A better upper bound**
Let PP be the class of promise problems $L = (L_y, L_n)$ that can be decided by a polynomial-time classical algorithm with success probability $> 1/2$ (meaning that for inputs $x \in L_y$ the algorithm accepts with probability $> 1/2$, and for $x \in L_n$ it accepts with probability $< 1/2$). Verify that PP $\subseteq$ PSPACE. Show that QMA $\subseteq$ PP. *[Hint: first show that* QMA $\subseteq$ PQP*, which is the same as* PP *but the algorithm is allowed to be quantum.]*