Quantum Proofs, Semester A 2024

Homework # 1 Solutions **January 4, 2024**

Rather than complete solutions, I indicate the main ideas for questions that created difficulties. A complete solution, earning full points, would have more details in the calculations and so would probably run an additional 2-3 pages in total. (When describing a circuit, some of you drew a picture, which is perfectly appropriate. You are always welcome to include a picture of hand-drawn circuit; which can be attached on a separate page if it is more convenient.)

Please read the document and check your understanding of the answer. If you feel that your solution was correct, but I mistakenly did not award you all points, please talk to me. If my sketch is not detailed enough and you would like to see a full solution, please ask me as well.

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 $\frac{1}{3}$).

   The first two questions were solved correctly by almost everyone. A possible way of defining A is as
   $$A = (\mathbb{I} \otimes \langle 0|_A)U(\mathbb{I} \otimes |1\rangle\langle 1|_O)U^\dagger(\mathbb{I} \otimes |0\rangle_A) , \qquad (1)$$
   where we have labeled the single-qubit output register as "O" and the m-qubit ancilla register as "A". Then A is a $2^q \times 2^q$-dimensional matrix, which is positive definite as the conjugation of a projection, $\mathbb{I} \otimes |1\rangle\langle 1|_O$ which is positive semidefinite, by a unitary, U, and a rectangular matrix, $\mathbb{I} \otimes \langle 0|_A$.

   (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 $\mathsf{QMA} \subseteq \mathsf{PSPACE}$. 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.

   This part could be done with various levels of care. Here is the main idea. Note that U has a decomposition $U = G_T \cdots G_1$ as a product of one- or two-qubit gates

$G_1, \ldots, G_T$. Now, we can write

$$\begin{aligned}\mathrm{Tr}(A^t) &= \mathrm{Tr}(A \cdots A) \\ &= \sum_{x_1 \in \{0,1\}^q} \langle x_1 | A \cdots A | x_1 \rangle \\ &= \sum_{x_1, \ldots, x_t \in \{0,1\}^q} \langle x_1 | A | x_2 \rangle \langle x_2 | A | x_3 \rangle \cdots \langle x_t | A | x_1 \rangle \ .\end{aligned}$$

This is simply because the trace can be computed by summing diagonal coefficients in any basis; and because $\mathbb{I} = \sum_x |x\rangle\langle x|$. Now if we write out the formula defining A (1) and again introduce resolutions of the identity at each step, we obtain an expression that looks like

$$\mathrm{Tr}(A^t) = \sum_{x_1, \ldots} \langle x_1 | \cdots | x_j \rangle \langle x_j | G_k | x_{j+1} \rangle \langle x_{j+1} | G_{k-1} | x_{j+2} \rangle \langle x_{j+2} | \cdots | x_1 \rangle \ ,$$

where the point is that we introduced resolutions of $\mathbb{I}$ between any two elementary gates. Finally, one needs to observe that the right-hand side can be evaluated in PSPACE, using a counter for each of the polynomially variables x_j, and such that each term in the sum can be computed in polynomial space by multiplying the appropriate matrix coefficients. (Most terms of the form $\langle x_j | G_k | x_{j+1} \rangle$ will be equal to 0, because if x_j and x_{j+1} differ on a bit on which G_k acts as identity, we get zero; nevertheless, the important point is that any such term can be easily computed given a 4×4 matrix representation for the 2-qubit gate G_k.)

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 $b - a > 1/\mathrm{poly}(n)$, the problem (a, b)-NIC is in QMA.

   We need to design a verification circuit. The verification circuit uses a single ancilla qubit initialized in state $|0\rangle$, and m proof qubits, where recall that m is the number of qubits that U acts on. The verification circuit can be expressed as $V = (\mathbb{I} \otimes X_A)(\mathbb{I} \otimes H_A) CTL_A U (\mathbb{I} \otimes H_A)$. Here, $CTL_A U$ designates the application of U, controlled on the ancilla qubit; and X_A and H_A denote application of a single-qubit X and H gates on qubit A respectively. The output qubit is the qubit in A. For any proof state $|\psi\rangle$, the probability that the output qubit of $V|\psi\rangle|0\rangle_A$ is 1 is calculated to equal

$$\frac{1}{4} \big\| |\psi\rangle - U|\psi\rangle \big\|^2 \ .$$

From there, completeness and soundness parameters can be determined to equal $\frac{1}{4}a^2$ and $\frac{1}{4}b^2$ respectively.

(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.]*

We use the hint, but it should be completed by introducing a similar "trick" to deal with ancilla qubits. Let V be a (unitary) QMA verification circuit with q proof qubits, labeled Q, and m ancilla qubits, labeled A. We also let O denote the output qubit. Let's assume that this circuit has been amplified, so that c is exponentially close to 1, and s exponentially close to 0.

Consider the following $(q + m + 1)$-qubit unitary, where the additional qubit is labeled B:

$$U_{AQB} = V^\dagger \cdot C_O R_B \cdot V \cdot C_A R_B \; .$$

Here, $C_A R_B$ applies a small rotation, of some angle θ (say $\theta = \pi/8$), on qubit B, controlled on A *not* being in state $|0\rangle_A$; and $C_O R_B$ applies the same rotation on qubit B, controlled on qubit O being in state $|0\rangle_O$. V and $V^\dagger$ both act as identity on B.

We can verify that for $|\psi\rangle$ a proof that is accepted by V with high probability, $U_{AQB}|\psi\rangle_Q|0\rangle_A|0\rangle_B \approx |\psi\rangle_Q|0\rangle_A|0\rangle_B$, up to exponentially small corrections. This is because neither of the controlled-operators is "triggered" by this input state, and so the whole circuit acts (more or less) as the identity.

The soundness case is more difficult. Suppose that V rejects all states with probability exponentially close to 1. We decompose an arbitrary state $|\psi\rangle_{QAB}$ on which U_{AQB} can act as

$$|\psi\rangle_{QAB} = |\psi_0\rangle_{QB}|0\rangle_A + |\psi_1\rangle_{QB}|\phi\rangle_A \; ,$$

where $|\phi\rangle_A$ is orthogonal to the all-0 state. States of the form $|\psi_1\rangle_{QB}|\phi\rangle_A$ have their qubit B rotated by the first $C_A R_B$, and nothing in the remaining circuit will bring them back close to their original state. States of the form $|\psi_0\rangle_{QB}|0\rangle_A$ have their qubit B rotated by the second $C_O R_B$, because they are very close to having their O qubit set to 1 after application of V, by the soundness assumption.

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 $\delta = \frac{1}{3}2^{-q(n)}$.

This is a direct application of sequential soundness amplification.

(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 $\frac{1}{3}2^{-q(n)}$.

Everyone solved this correctly; noting that in the case $x \in L_y$ we in fact have a slightly better bound of $2^{-q}(1 - \frac{1}{3}2^{-q})$. This part uses that running the verification circuit on a uniformly random basis state is *equivalent* to running it on a uniformly random state from *any* orthonormal basis — such as a basis that contains an optimal proof state as one of its elements. (Indeed, the density matrix that represents either mixture is the totally mixed state, i.e. the (scaled) identity matrix.)

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

Containment of BQP is clear. For the reverse inclusion, we note that a BQP algorithm can easily prepare the totally mixed state on q qubits, for example by preparing q EPR pair in parallel and acting on one half of each pair. Using that $q = O(\log n)$, the gap between the two cases in the previous question is inverse polynomial, which can be amplified by sequential repetition of the BQP algorithm.