Frontiers of Quantum complexity *Instructors: Anand Natarajan, Anurag Anshu*

Problem set 1

Due: Thu, Oct 9, 2025 *TFs: Yeongwoo Hwang, Tina Zhang*

Instructions

You may work with collaborators and consult textbooks or other references, but please list your collaborators and cite any references you use.

Background

The *von Neumann entropy* of a quantum state ρ is defined as $\mathrm{S}(\rho) = -\mathrm{Tr}(\rho \log \rho)$. Umegaki's *relative entropy* between two quantum states ρ, σ is defined as $\mathrm{D}(\rho \| \sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma)$.

Symmetric subspace: given two systems A, B (with isomorphic Hilbert spaces $\mathcal{H}$) of dimension d each, the symmetric subspace is $\Pi_{sym} = \mathrm{span}\{|\psi\rangle_A \otimes |\psi\rangle_B, \forall |\psi\rangle \in \mathcal{H}\}$. The swap test (see problem set 0) checks whether a vector is in the symmetric subspace. In other words, $\Pi_{sym} = \frac{\mathbb{1} + \mathrm{Swap}_{A,B}}{2}$.

Q1: PP and friends (6 points)

In class we didn't quite finish the proof that $\mathsf{QMA} \subseteq \mathsf{PP}$. Let's deal with some of the loose ends now.

(a) **(1 point)** We say a function $f : \{0,1\}^* \to \mathbb{Z}$ is in GapP if there is a Turing machine M such that $f(x)$ is equal to the difference between the number of accepting and rejecting paths of M. (If you prefer to think about randomized algorithms, $f(x)$ is the difference between the number of random seeds that case the algorithm M to output YES and NO).

Suppose f and g are GapP-computable functions. Show that $h(x) = f(x)g(x)$ is also in GapP.

(b) **(2 points)** Suppose we have two $2^n \times 2^n$ matrices $A^{(n)}, B^{(n)}$ whose entries are all computable in GapP: that is, the functions $f(i,j) = A^{(n)}_{ij}$ and $g(i,j) = B^{(n)}_{ij}$ are in GapP. Show that the entries of

$$C^{(n)} = A^{(n)} B^{(n)}$$

are computable in GapP as well.

(c) **(2 points)** Let $U = U_1 \dots U_t$ be the unitary corresponding to a quantum circuit built out of gates $U_1, \dots, U_t$. The entries of U cannot be GapP functions, since they are not integers in general. Show nonetheless that if the circuit is built out of Hadamard and Toffoli gates only, that each entry of U can be written as

$$U_{ij} = \frac{f(i,j)}{\sqrt{2^{k(n)}}},$$

where $k(n)$ is efficiently computable and $0 \leq k(n) \leq t$.

(d) **(1 point)** Argue that, given a QMA verifier circuit, there exists a GapP function f and an efficiently computable $k(n) = \mathrm{poly}(n)$ such that

- If x is a YES instance, then $f(x) \geq 0.9 \cdot 2^{k(n)}$.

- If x is a NO instance, then $f(x) \leq 0.1 \cdot 2^{k(n)}$.

(Hint: consider the acceptance probability of the circuit on a random input, as discussed in class.) From here, it's not too hard to obtain containment in PP (but you do not need to do it here).

Q2: Circuit-to-Hamiltonian for simple quantum circuits (5 points)

Here we will look at circuit-to-Hamiltonian mappings for simple classes of quantum circuits, and try to understand why they do not generalize to general quantum circuits. This helps us appreciate the power of the Feynman-Kitaev mapping.

(a) **(1 point)** Suppose $U = U_1 \ldots U_T$ is a quantum circuit of depth d on n qubits, that is $U = V_1 V_2 \ldots V_d$, where V_i is a layer of gates on n qubits in which no two gates overlap. Consider the state $U \left|0\right\rangle^n$. Show that this state is the unique ground state of the Hamiltonian $H_U = \sum_i U \left|1\right\rangle\!\left\langle 1\right|_i U^\dagger$.

(b) **(1 point)** In the above construction, what is the locality of the Hamiltonian H_U? What is the spectral gap of H_U? Why is H_U not a good option for QMA-completeness of the local Hamiltonian problem?

(c) **(1 point)** Next, consider a quantum circuit $W = W_1 \ldots W_T$ on a d dimensional quantum system $\mathcal{H}_S$. Consider the quantum state $W\left|0\right\rangle$, where $\left|0\right\rangle$ is a fixed state in $\mathcal{H}_S$. Introduce $T+1$ copies of $\mathcal{H}_S$, labelled $S_0, S_1 \ldots S_T$, and consider the Hamiltonian

$$H_W = \sum_{i=0}^{T-1} (\mathbb{1} \otimes W_{S_{i+1}}) \Pi_{sym,S_i,S_{i+1}} (\mathbb{1} \otimes W^\dagger_{S_{i+1}}).$$

Prove that the ground space of H_W is

$$\mathrm{span}\{\left|\psi\right\rangle_{S_0} \otimes W_1 \left|\psi\right\rangle_{S_1} \otimes W_2 W_1 \left|\psi\right\rangle_{S_2} \otimes \ldots (W_T \ldots W_1) \left|\psi\right\rangle_{S_T}, \forall \psi \in \mathcal{H}_S\}.$$

(d) **(1 point)** Write down the ground space of $(\mathbb{1} - \left|0\right\rangle\!\left\langle 0\right|)_{S_0} + H_W$.

(e) **(1 point)** If S consists of n qubits ($d = 2^n$) and W_i are 2-qubit gates, what is the locality of H_W? Why is $(\mathbb{1} - \left|0\right\rangle\!\left\langle 0\right|)_{S_0} + H_W$ not a good option for QMA-completeness of the local Hamiltonian problem?

Q3: Jaynes' principle (3 points)

Jaynes' principle is an idea from statistical inference, which says that we should model an unknown system by the maximum entropy distribution consistent with our observations of the system. The quantum Gibbs state has an elegant interpretation as the maximum entropy state subject to observational constraints. Consider a collection of Hermitian operators $E_1, E_2, \ldots E_m$. Suppose ρ is an unknown quantum state with the promise that $\mathrm{Tr}\left(\rho E_i\right) = \mu_i$ for all i. Then the quantum Gibbs state

$$\rho_{\text{Gibbs}} := \frac{e^{-\sum_i \lambda_i E_i}}{\mathrm{Tr}\left(e^{-\sum_i \lambda_i E_i}\right)},$$

for some λ_i that satisfy $\mathrm{Tr}\left(E_i \rho_{\text{Gibbs}}\right) = \mu_i$ is the unique maximizer for $\mathrm{S}\left(\rho\right)$. We will prove this in the following questions.

Let's abbreviate $Z = \mathrm{Tr}\left(e^{-\sum_i \lambda_i E_i}\right)$ as the quantum partition function.

(a) (2 points) For any quantum state ρ, show that $\mathrm{D}\left(\rho \| \rho_{\mathrm{Gibbs}}\right) = S(\rho_{\mathrm{Gibbs}}) - S(\rho)$.

(b) (1 point) Use the non-negativity of relative entropy to show that $\mathrm{S}\left(\rho\right) \leq \mathrm{S}\left(\rho_{\mathrm{Gibbs}}\right)$. Show that equality is achieved iff $\rho = \rho_{\mathrm{Gibbs}}$.

Jaynes' principle makes (quantum) Gibbs states as a crucial concept in (quantum) learning theory, allowing their use as a natural ansatz for an unknown (quantum) state, subject to experimentally observable constraints. In fact, this is the reason why the Boltzmann distribution shows up in statistical mechanics—it is exactly how Jaynes' principle tells us to describe the unknown state of $O(10^{23})$ atoms given only the observed values of macroscopic quantities like pressure, volume etc.