2.111/8.370/18.435 Problem Set 8 Solutions

Due: November 26, 2015

1. **(Graph Isomorphism)**

   A graph g with n vertices and m edges is specified by a list of the edges $\{(i_1, j_1), (i_2, j_2), \ldots, (i_m, j_m)\}$, given in some standard order (e.g., start with the lowest numbered index for both).

   A permutation $\pi \in S_n$, where S_n is the symmetric group, is a one to one mapping from the set of vertices onto itself. There are $n!$ permutations in the group.

   Define the action of a permutation on the graph, $\pi(g)$, by its action on the list,

   $$\pi(g) = R\{(\pi(i_1), \pi(j_1)), (\pi(i_2), \pi(j_2)), \ldots, (\pi(i_m), \pi(j_m))\},$$

   where R indicates that the list has been reordered to conform to the standard order.

   Consider two graphs g_1,g_2, with the same number of vertices and edges. The problem is to determine whether g_1 and g_2 are isomorphic, i.e., does there exist a π_0 such that $\pi_0(g_1) = g_2$?

   A quantum computer can be used to construct the state

   $$|\psi_1\rangle = \frac{1}{\sqrt{n!}} \sum_{\pi \in S_n} |\pi\rangle_A \otimes |\pi(g_1)\rangle_B.$$

   The state $|\psi_2\rangle$ can be constructed similarly.

   The reduced density matrix for the B subsystem for $|\psi_1\rangle$ is $\rho_1^B = \mathrm{tr}_A |\psi_1\rangle\langle\psi_1|$. Similarly for ρ_2^B.

   Part 1 of the problem is to show that the explicit form of ρ_1^B is $(1/n!) \sum_\pi |\pi(g_1)\rangle\langle\pi(g_1)|$. Similarly for ρ_2^B. (Prove this.)

   The Hilbert space of A is spanned by basis states corresponding to permutations $\pi \in S_n$, so $\langle\pi|\pi'\rangle = \delta_{\pi\pi'}$:

   $$\rho_1^B = \mathrm{tr}_A |\psi_1\rangle\langle\psi_1| = \frac{1}{n!} \mathrm{tr}_A \sum_{\pi, \pi' \in S_n} |\pi\rangle_A \langle\pi'| \otimes |\pi(g_1)\rangle_B \langle\pi'(g_1)| = \frac{1}{n!} \sum_{\pi \in S_n} |\pi(g_1)\rangle\langle\pi(g_1)|.$$

   Similarly,

   $$\rho_2^B = \mathrm{tr}_A |\psi_1\rangle\langle\psi_1| = \frac{1}{n!} \mathrm{tr}_A \sum_{\pi, \pi' \in S_n} |\pi\rangle_A \langle\pi'| \otimes |\pi(g_2)\rangle_B \langle\pi'(g_2)| = \frac{1}{n!} \sum_{\pi \in S_n} |\pi(g_2)\rangle\langle\pi(g_2)|.$$

   When does $\rho_1^B = \rho_2^B$? (Hint: compare the situations when g_1, g_2 are isomorphic, and then they are not.)

   If g_1 and g_2 are isomorphic, there exists a $\pi_{12} \in S_n$ such that $\pi_{12}(g_1) = g_2$. The set $\{\pi(g_2)\}_{\text{all } \pi \in S_n} = \{\pi(\pi_{12}(g_1))\}_{\text{all } \pi \in S_n} = \{\pi(g_1)\}_{\text{all } \pi \in S_n}$. So $\rho_1^B = \rho_2^B$.

   If g_1 and g_2 are not isomorphic, $\{\pi(g_1)\}_{\text{all } \pi \in S_n}$ and $\{\pi(g_2)\}_{\text{all } \pi \in S_n}$ are disjoint. So ρ_1^B and ρ_2^B have disjoint supports.

If so, does this allow one to solve the graph isomorphism problem? That is, is there a measurement that one can make on multiple copies of ρ_1^B, ρ_2^B that will determine whether or not g_1 and g_2 are isomorphic? If so, how many times must this measurement be performed?

What you are expected to argue (or exhibit some intuition) is that a small number of measurements (more precisely, poly(n)) does not suffice to tell if any $\rho_1^B = \rho_2^B$ with high probability. The main idea can go as follows. By making one measurement on ρ_1^B or ρ_2^B you observe one basis state of their supports, which are typically $O(n!)$-dimensional (superexponentially large). Your goal is to tell if the two supports are spanned by the same set or disjoint sets of $O(n!)$ basis states. In either case $O(n!)$ measurements are necessary for a $1/2 + c$ success probability where c can be a constant, since in the large n limit, $o(n!)$ measurements can only traverse a vanishingly small subspace. For example, if $\rho_1^B = \rho_2^B$ (isomorphic), the scenario is basically the following: you have two identical lists of $O(n!)$ different numbers, but you can randomly query only a vanishingly small number of elements from each. Obviously the probability that you get two same numbers is vanishingly small. Similarly for the non-isomorphic case.

That is, this algorithm cannot solve GI *efficiently*. (The recent breakthrough by Babai is that GI can be solved classically in quasipolynomial time.)

2. **Find continued fractions for $\pi, e, \sqrt{2}$. Construct the first 5 truncated rational approximations.**

   We denote each continued fraction $a_0 + \frac{1}{a_1 + \cdots}$ as an ordered list of integers $\{a_0; a_1, \cdots\}$.

$$\pi = \{3; 7, 15, 1, 292, 1, \cdots\} \approx \frac{104348}{33215} \approx 3.14159.$$

$$e = \{2; 1, 2, 1, 1, 4, \cdots\} \approx \frac{87}{32} = 2.71875.$$

$$\sqrt{2} = \{1; 2, 2, 2, 2, 2, \cdots\} \approx \frac{99}{70} \approx 1.41429.$$