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 $\rho_1^B = \mathrm{tr}_A |\psi_1\rangle\langle\psi_2|$. Similarly for ρ_2^B.

Part 1 of the problem is to show that the explicit form of ρ_1^B is $(1/n!) \sum_\pi |\pi(g_1)\rangle\langle\pi(g_2)|$. Similarly for ρ_2^B. (Prove this.)

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 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?