Homework 5: Problem 5

William Svoboda (wsvoboda)

Collaborators: Epi Torres-Smith, Leslie Kim

Problem 5:
We wish to show that if Alice follows the given protocol Bob can derive a valid 3-coloring of G in poly-time.

While only Alice knows the color of each vertex, Bob still has knowledge of the edge set and vertex set of G. Furthermore, Bob can still fail to derive a valid coloring in poly-time if he decides to only pick the same two vertices each round (or a variation of this action) without ever testing any of the other vertices. From this observation, we will describe a two-step algorithm that Bob can use to always derive a valid coloring (assuming that G is indeed 3-colorable).

1. In the first step, we observe that vertices of the same color belong to the same set no matter what that color actually is. While Alice permutes the colors of G randomly each round, which prevents Bob from gaining knowledge of the actual coloring, it does not change the three sets that make up the coloring. To reconstruct these sets, Bob can test every vertex in G with every other vertex in the graph. If the second vertex considered has the same color, Bob marks them as being in the same set. This operation takes time proportional to $O(n^2)$.

2. In the second step, Bob can assign a unique color to each of the sets. In the first step, Bob can reject G if Alice ever revealed to him a vertex with a fourth color that would make the graph not 3-colored. However, to be sure his derived coloring is valid, Bob still needs to explicitly check each pair. By the definition of a graph coloring, a coloring is only valid if adjacent vertices never share the same color. Checking each pair also takes time proportional to $O(n^2)$, and by the end Bob can be sure he has a valid coloring if none of the pairs share the same color.

Because both steps take time proportional to $O(n^2)$, we have shown that Bob can derive a valid 3-coloring of G in poly-time using the given protocol.