CSE P531: Computability and Complexity Theory (Spring, 2016)

Homework 5 Out: Thursday, 28-Apr. **Due**: Saturday, 7-May (9pm in the **Dropbox**)

Reading:

Sipser, 7.4—7.5; Arora-Barak 2.2—2.4

Instructions:

Your proofs and explanations should be clear, well-organized and as concise as possible.

You are allowed to discuss the problems with fellow students taking the class. However, you must write up your solutions completely on your own. Moreover, if you do discuss the problems with someone else, I am asking, on your honor, that you do not take any written material away from the discussion. In addition, for each problem on the homework, I ask that you acknowledge the people you discussed that problem with, if any.

Most of the problems require only one or two key ideas for their solution – spelling out these ideas should give you most of the credit for the problem even if you err in some finer details. So, make sure you clearly write down the main idea(s) behind your solution.

A final piece of advice: Begin work on the problem set early and don't wait until the deadline is only a few days away.

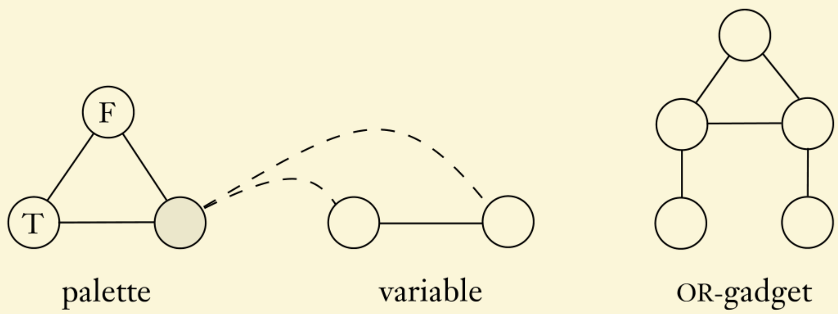
1. Graph coloring

Problem 7.29 from Sipser:

7.29 A ***coloring*** of a graph is an assignment of colors to its nodes so that no two adjacent nodes are assigned the same color. Let

$$3COLOR = \{\langle G \rangle \mid G \text{ is colorable with 3 colors}\}.$$

Show that *3COLOR* is NP-complete. (Hint: Use the following three subgraphs.)



2. 3-Coloring planar graphs

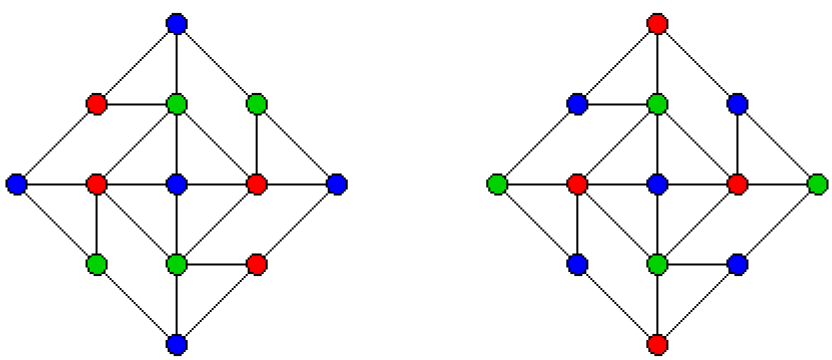
Recall the graph 3-coloring problem from Exercise #1:

$$\text{3-COL} = \{ \langle G \rangle : G \text{ is a 3-colorable graph } \}$$

A graph is called **planar** if the vertices can be drawn as points in the plane and the edges as straight lines such that two distinct edges in the drawing do not cross (they may meet at their endpoints, of course).

$$\text{PLANAR-3-COL} = \{\langle G \rangle : G \text{ is a planar 3-colorable graph } \}$$

Your goal is to prove that 3-COL $\leq_P$ PLANAR-3-COL, thereby proving that PLANAR-3COL is NP-complete. You should use the following gadget to uncross edges:



Do the problem in three parts:

(a) Given colors $c_1, c_2 \in \{R, G, B\}$, observe that there is always a way to 3-color the graph so that the opposite east-west corners are colored c_1 and the opposite north-south corners are colored c_2. Note that possibly $c_1 = c_2$. (That this is true follows from the two colorings given above.)

(b) Show that **any** 3-coloring of the gadget must have the property that opposite corners have the same color.

(c) Use this to reduce 3-COL to PLANAR-3-COL. Remember that if the edges x-y and u-v cross, then the gadget should remove the edge crossing, but enforce the same constraints that x/y must be colored differently and u/v must be colored differently.

Extra credit [worth 2 regular problems]:

Prove that if P=NP, then you can break the RSA cryptosystem

[http://en.wikipedia.org/wiki/RSA_(cryptosystem)]

In other words, show that given someone's public key, you can compute their private key in polynomial time.