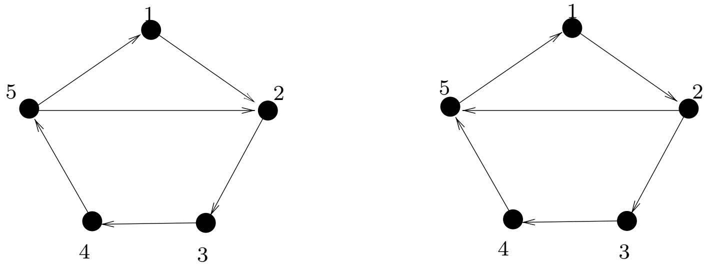
Honors Theory, Spring 2002, Yap
Homework 6

This is due on Wed April 17.
All reducibility concepts assume Karp-reducibility.

1. (15 Points) The proof of Cook's theorem in Chapter 3 reduces any language $A \in NP$ to SAT. If M is an NP-machine for A, for any input w, the proof constructs a 3CNF formula F_w such that F_w is satisfiable iff $w \in A$. We claim that something stronger is true: $\#(F_w)$ is equal to the number of accepting computations of M on input w. Actually, this claim needs a mild condition on M. What is it? Prove this claim under this mild condition. **Hint:** if you do not see what this condition might be, we suggest the strategy of ignoring it at first, and trying to prove the claim unconditionally.

2. (20 Points) Prove that QBF is $PSPACE$-complete. Since this proof can be found in the literature, I will enforce some originality in your solution by asking you to use the same framework as my description of Cook's theorem in Chapter 3. The additional idea you need comes from the key idea in the proof of Savage's theorem: if $C \vdash^{2m} C'$ (i.e., there is an $2m$-step path from C to C' then $C \vdash^{m} C''$ and $C'' \vdash^{m} C'$ for some C''.

3. (20 Points) This exercise helps you gain some facility with the group theoretic ideas in the NONISO $\in$ IP proof. Let $V = V_n = \{1, \ldots, n\}$ and S_n be the set of permutations on V_n. The trivial permutation is denoted $\mathbf{1}_n$ (or simply $\mathbf{1}$). Write the composition of $\sigma, \sigma' \in S_n$ in the form of a product $\sigma\sigma'$, instead of $\sigma \circ \sigma'$.
(i) Let $2 \leq k \leq n$. If $\{a_1, \ldots, a_k\} \subseteq \binom{V}{k}$, then $(a_1, \ldots, a_k) \in S_n$ denotes the permutation which takes each a_i to $a_{(i+1 \bmod k)}$, called a **cyclic permutation**. Two special cases are $k = 2$ or $k = n$. Then $(a_1, \ldots, a_k)$ is **transpose** or a **Hamiltonian permutation**, respectively. Two cyclic permutations $(a_1, \ldots, a_k)$, $(b_1, \ldots, b_\ell)$ are disjoint if $a_i \neq b_j$ for all i, j. For instance, $(132)(45) = (45)(132)$ is a product of two disjoint cycles. The order of writing disjoint products does not matter. Show that every non-trivial permutation is a product of disjoint permutations.



(a) G_0

(a) G_1

Figure 1: Two labeled digraphs G_0, G_1.

(ii) Let G_0 be the digraph shown in Figure 1. Determine $\mathtt{iso}(G_0)$ and $\mathtt{iso}(G_1)$. What the sizes of these two sets?
(iii) Determine $\mathtt{aut}(G_0)$ and $\mathtt{aut}(G_1)$. What the sizes of these two sets?