Computer Science 340
Reasoning about Computation
Princeton University, Fall 2020

Assignment 5 Handout
Due 12/2/2020, 9:00PM

Problem 1 [20 points]
Let $G(V, E)$ be a simple graph. As a reminder, we say that G is k-**colorable** if we can color the vertices of G using at most k colors, such that no two adjacent vertices get the same color.
Prove that 4-**colorability** is NP-complete.
(Hint: You may assume that 3-colorability is NP-complete)

Problem 2 [20 points]
Consider the following two decision problems

- DISJOINT_PATHS(G, s, t, k), where $G = (V, E)$ is a simple graph, $s, t \in V$ and $k \in \mathbb{N}$. Are there k disjoint paths connecting s and t? By "disjoint paths connecting s and t" we mean paths that share no vertices apart from s, t.

- PERFECT_MATCHING(G, A, B), where G is a simple, bipartite graph, with parts A and B, such that $|A| = |B|$. Does G have a perfect matching?

Show the reduction PERFECT_MATCHING$\leq_p$DISJOINT_PATHS.
(As a reminder, $\leq_P$ denotes a Karp reduction)

Problem 3 [20 points]
Find the following values. Provide a proof that your answers are correct.
(A) Compute $3^n \pmod{11}$ for $n = 1, 2, \ldots, 10$.

(B) What is the value of

$$3^{232423894234872138124 5} \mod 11?$$

(C) What is the value of

$$15^{3248723482156246732128312537123} \mod 11?$$

Problem 4 [20 points]

Consider the Euclidean Algorithm for computing the greatest common divisor of two integers $a \geq b > 0$, namely $gcd(a, b)$.

Algorithm 1 EUCLID(a, b)

```
    Input: Integers $a, b$ such that $a \geq b > 0$
    Output: gcd$(a, b)$
if $b|a$ then
    return $b$
else
    return EUCLID$(b, a \mod b)$
```

Assume that we want to calculate $\gcd(a_0, b_0)$, with $a_0 \geq b_0 > 0$. Let ℓ the number of recursive calls of EUCLID to calculate $\gcd(a_0, b_0)$ and a_i, b_i be the argument to the ith recursive call of the algorithm EUCLID, where $i = 1, 2, \ldots, \ell$.

(A): Show that $b_{j+2} \leq b_j/2$, for $0 \leq j \leq \ell - 2$.

(Hint: You might want to consider the following the two complementary cases: if $b_{j+1} \leq b_j/2$ and if $b_{j+1} > b_j/2$.)

(B): Show that there are at most $2 \cdot \lfloor \log_2 b_0 \rfloor$ recursive calls to EUCLID. Note that the length of the binary representation of a positive integer x is $\lfloor \log_2 x \rfloor + 1$.

Problem 5 [20 points]

Given a graph $G = (V, E)$, with $n = |V|$, Alice has a 3-coloring of G with colors red, green and blue. Alice wants to convince Bob that G is 3-colorable via the following interactive protocol. In each round of the interaction, the following steps are repeated:

1. Bob leaves the room. Alice permutes the 3 colors in her coloring randomly (independently from any permutations that occured on previous rounds). To provide an example of such a permutation, Alice can switch red to blue, blue to green and green to red.

2. Alice covers all vertices of the graph G. Bob enters the room. As a result, Bob is not able to see the color of each vertex, unless Alice reveals it.

3. Bob picks any two vertices of his choice to be revealed. Alice reveals the colors of those vertices. If the two colors of those vertices are the same and the vertices are connected by an edge or if a color is revealed that is not blue, red or green, Bob rejects that round; otherwise Bob accepts. (Note: This is the step that is different from the Zero Knowledge proof protocol for 3-coloring mentioned in the Lectures)

Alice and Bob repeat the above 3 steps n^3 times. If in all those rounds Bob accepts, then Bob agrees that G is 3-colorable. Otherwise Bob rejects the notion that G is 3-colorable.
Assume that indeed G is 3-colorable. Show that if Alice does not wish to "cheat" and follows the protocol as stated, Bob can use the protocol above to derive a valid 3-coloring of G in poly-time.

Problem 6 [20 points]
Consider the decision problem HITTING-SET$(A, A_1, A_2, \ldots, A_m, k)$: "Given a set $A = \{x_1, x_2, \ldots, x_n\}$ of $n \geq 1$ elements, a collection of $m \geq 1$ subsets $A_1, A_2, \ldots A_m \subseteq A$ of the set A, and an integer $k \geq 1$, is there a set $H \subseteq A$

of size k that contains at least one element of each A_i, namely $H \cap A_i \neq \emptyset$ for all $i = 1, 2, \ldots, m$?

Show that the HITTING-SET decision problem is NP-complete.

(Hint: You may find the fact that the VERTEX-COVER decision problem is NP-complete helpful. For reference, VERTEX-COVER(G, ℓ): "Does the undirected graph $G = (V, E)$ have a vertex cover of size ℓ?". Note that $\ell \geq 1$. Furthermore, a vertex cover of an undirected graph is a subset $V' \subseteq V$, such that if $(u, v) \in E$ then $u \in V'$ or $v \in V'$ or both and the size of a vertex cover is the number of vertices in it.)