HW10
Due: December 1, 2016

Attach a fully filled-in cover sheet to the front of your printed homework. Your name should not appear anywhere except on the cover sheet; each individual page of the homework should include your Banner ID instead.

While collaboration is encouraged in this class, please remember not to take away notes from any collaboration sessions. Also please list the names and logins of any of your collaborators at the beginning of each homework.

Please monitor Piazza, as we will post clarifications of questions there. You should hand in your solutions by 12:55 to the CSCI 1010 bin on the second floor of the CIT. Late homeworks are not accepted.

Problem 1

a. Define the symmetric difference (denoted by ⊕) between sets $A$ and $B$ as follows:

$$A ⊕ B = \{w \mid (w ∈ A \text{ and } w /∈ B) \text{ or } (w ∈ B \text{ and } w /∈ A)\}$$

This is also called the disjunctive union. Determine whether P, NP, and PSPACE are closed under symmetric difference. Prove each of your answers or relate it to an open problem.

b. Determine whether PSPACE is closed under the Kleene star operation. Prove your answer or relate it to an open problem.

Problem 2

Let $\text{ColorRange}$ be the language defined as follows:

$$\text{ColorRange} = \{(G, lo, hi) \mid hi ≥ lo ≥ 0, \begin{align*}
G \text{ is a } k\text{-colorable graph with } k ≤ hi, \\
G \text{ is not a } j\text{-colorable graph for } j < lo, \\
\text{and } hi \text{ and } lo \text{ are integers represented in binary}\end{align*}\}$$

a. Show that $\text{ColorRange}$ is in PSPACE.
b. Show that \textsc{ColorRange} is NP-hard.

c. Show that \textsc{ColorRange} is coNP-hard.

d. Show that if \textsc{ColorRange} is in NP, then NP = coNP.

\textbf{Problem 3}

A language $L$ is in LOGSPACE if there exists a TM $M$ that decides $L$ using space only logarithmic in the size of the input. $M$ is allowed to read all of its input (taking linear time) but cannot alter more than a logarithmic portion of the tape. If we think of $M$ as a two-tape TM, then one read-only tape contains the input, and one writable tape is $M$’s work tape. By this definition, $L$ is in LOGSPACE if $M$ writes to a portion of the work tape that is $O(\log n)$ where $n$ is the size of the input.

Let $A$ be the language of matching parentheses. For example “((()” and “((()())” are in $A$, but “))” is not. Show that $A$ is in LOGSPACE.

\textbf{The following questions are lab problems.}

\textbf{Lab Problem 1}

Ginger O’Nion is wracked with anxiety that her soulmate, Rudy Bega, may have betrayed her. How else could Walter Chestnutt have gotten her family’s mangelwurzel secrets? To exacerbate her suspicions, Rudy has been sending encrypted love letters and who knows what other kinds of secret messages.

Ginger knows that it is an open question as to whether P = NP. If P = NP, there would be efficient ways to solve so many hard problems: rotating crops, planning a tour of every batata farm in the country, moving turmeric distribution sites, distributing fertilizer—the list goes on. However, while making hard problems easy would be helpful in some areas of society, there are other areas that depend on the existence of hard problems. One such area is the field of cryptography.

In general, we want it to be hard for people to read secret messages, but if all of NP suddenly became easy, then deciphering messages might become easy.

\footnote{Think about what would be “easy” if we had polynomial time algorithms to NP-hard problems.}
as well. In this moment, Ginger is so upset with Rudy that she is ignoring all of the potentially catastrophic repercussions of P = NP, and is thinking only of what would happen if she could read Rudy’s messages.

Rudy’s method of encryption relies on a cryptographic primitive that could not exist if P = NP: one-way functions. A one-way function is a function that is easy to compute but hard to invert, which is why we call it ‘one-way’. (You can imagine why an operation that is easy to perform but difficult to reverse would be useful in cryptography, and in aiding a cheating lover in their infidelity.) Specifically, Rudy’s encryption method relies on one-way functions over binary strings, where the length of the output is the same as the length of the input.

**Definition**: A function \( f : \{0,1\}^* \rightarrow \{0,1\}^* \) is a **one-way function** if:

- For all \( x \in \{0,1\}^* \), \( |x| = |f(x)| \).
- \( f \) is a polynomial-time computable function. Recall that this means there exists a polynomial-time TM \( M \) that halts with just \( f(x) \) on its tape, when started on any input \( x \in \{0,1\}^* \).
- There does not exist a polynomial-time TM \( A \) that on any input \( y \), outputs some \( x' \) such that \( f(x') = y \) if it exists.

An example of such a function is multiplication: while there is a polynomial-time procedure that takes as input two \( k \)-bit integers and computes their \( 2k \)-bit product, we do not know of a polynomial-time algorithm that takes as input a \( 2k \)-bit integer and, in polynomial time, finds its \( k \)-bit factors if they exist.

a. Consider the following language for a one-way function \( f \):

\[
\text{INVERSE}\text{SUFFIX}_f = \{ \langle y, w \rangle \mid y = f(x) \text{ for some } x \in \{0,1\}^*, \text{ and } w \text{ is the suffix (not necessarily proper) of some inverse of } y. \}
\]

That is, for some \( w' \in \{0,1\}^* \), \( f(w' \circ w) = y \)

Prove that for any one-way function \( f \), \( \text{INVERSE}\text{SUFFIX}_f \) is in NP.

b. Prove that if P = NP, then no one-way function can exist. That is, prove that if \( f : \{0,1\}^* \rightarrow \{0,1\}^* \) is a function such that \( |x| = |f(x)| \) for all

\(^2\)This definition is a simplified version of the standard cryptographic definition.
$x$ and $f$ is polynomial-time computable, then there exists a polynomial-time TM $A$ that on any input $y$, outputs some $x'$ such that $f(x') = y$ if it exists, and fails otherwise.

**Lab Problem 2**

Ginger intercepts another message from Rudy to Walter, which she suspects contains incriminating evidence regarding Walter Chestnutt’s trial. Walter Chestnutt has apparently been using his political campaign as a cover to obtain coveted agricultural secrets from unsuspecting farmers. His entire operation revolves around illegally brewing rootbeer, a concoction of man-gelwurzel and turmeric, through obfuscated recipes. Rudy has also been behaving really strangely, lately—well, even more so than a cheating lover would. He didn’t even know what TAUTOLOGY was, and that was their special language!

Ginger has seen Rudy building word ladders in his spare time, so she suspects that he and Walter Chestnutt are communicating using these word encryptions. A ladder is a sequence of strings $s_1, \ldots, s_k$ such that every string differs from the preceding string by exactly one character and all strings are of the same length. For example, the following is a ladder of English words, starting with ‘head’ and ending with ‘free’: head, hear, near, fear, bear, beer, deer, deed, feed, feet, fret, free. More formally:

$$\text{LADDERS} = \{ (D, s, t) \mid D \text{ is a DFA over } \Sigma \text{ and } L(D) \text{ contains a ladder of strings, starting with string } s \in \Sigma^* \text{ and ending with string } t \in \Sigma^* \}$$

Ginger needs your help to determine whether Rudy’s message is in the language LADDERS.

a. Give a ladder from ‘beet’ to ‘yuca’ using only common English words. (No proper nouns allowed!)

b. Show that LADDERS $\in$ PSPACE.
Lab Problem 3

Walter Chestnutt has been accused of a terrible crime: illegally obfuscating mangelwurzel and brewing rootbeer. This rare root vegetable is the sole property of the O’Nion family, who don’t look fondly on theft; if thieves get convicted, it’s a case of out of the frying pan and into the fire. The townsfolk of Myami shake their heads sadly, as they knew it was only a matter of time until that nut would get arrested. Walter insists that he is not a nut; he is a root vegetable, and the TAs\(^3\) just didn’t do a good enough job naming him to make that clear. “The problem is that a chestnut is such a well-known nut!” he squeals. “And Walter is too normal of a name for people to realize it’s just a pun on ‘water!’” Tired of hearing his incessant grumbling, the townsfolk decide that if Walter is convicted, he will not only be sent to jail and stripped of his farm, but his first name will be forcibly removed to demote him to a nut—forever.

Luckily for Walter, the townsfolk of Myami have a custom of playing a two-player game called LOSINGSUBSET. Like a bloodless version of trial by combat, the game puts everything Walter cares about at stake: his livelihood, his pride, and, most importantly, his root vegetable identity.

The game is based on a directed graph, and the rules are as follows:

- At the beginning of the game, a certain node \(s\) of the graph \(G\) is colored green.
- The two players take turns picking a neighboring uncolored node to the green node. It becomes the new green node, and the previous green node is now colored red. (If the green is at node \(u\), it can only move to node \(v\) if \((u, v) \in E\) and if \(v\) is not red).
- There is a subset of nodes \(L \subset V(E)\). The first player to move onto a vertex that belongs to the subset \(L\) loses, and the other player wins.
- If the current player cannot make a move (because all neighboring nodes have been visited), and no one has lost yet, the game ends in a tie.

Show that determining whether the first player has a \textbf{winning} strategy (i.e. that Walter can avert this Waltergate disaster) in an arbitrary instance of

\(^3\) Taxonomists of Agriculture
the game \textsc{LosingSubset} is PSPACE-complete. A tie is not a win. Note that an instance of the game \textsc{LosingSubset} consists of a directed graph $G$, a starting vertex $s$, and a losing subset $L$.

\textbf{Hint}: Recall from class the PSPACE-complete problem \textsc{Generalized-Geography}. To remind you, \textsc{GeneralizedGeography} is played in the same manner as \textsc{LosingSubset}, with two players taking turns moving a pebble on a directed graph. A player loses if they cannot move the pebble anywhere (i.e. if all neighboring nodes have already been visited).