Computational Models - Exercise #6 solution sketch

1. First, it is clear that $L_p \in \mathcal{NP}$. Now, $L \leq_p L_p$ by the reduction $f(x) = \langle x, 0\rangle$.

2. (a) The claim is true. Let M be the TM that decides A and as B is nontrivial, let $y \in B$ and $z \notin B$. The reduction $f(x)$ simulates M on x. If M accepted it outputs y and if M rejected it outputs z. The fact that f is computable and preserves correctness is immediate.

   (b) The claim is false. Assume to the contrary that $H_{TM,\epsilon} \leq_m \{1\}$ (both languages are in $\mathcal{RE}$), so $H_{TM,\epsilon} \in \mathcal{R}$, in contradiction.

   (c) The claim is false. Let $C_2 = \{L \in \mathcal{RE} \mid \epsilon \in L\}$, so $L_{C_2} = A_{TM,\epsilon} \in \mathcal{RE}$. Let $C_1 = \{L \in \mathcal{RE} \mid |L| \text{ is infinite}\}$, so $L_{C_1} = L_\infty \notin \mathcal{RE}$. Thus, it cannot be that $L_{C_1} \leq_m L_{C_2}$.

   (d) The claim is false. Let $L' = \{w \in \{0,1\}^\star \mid \#_0(w) = \#_1(w)\}$ and let $C = \{L \in \mathcal{RE} \mid L \subseteq L'\}$. C is nontrivial, so $L_C = L_1 \notin \mathcal{R}$, by Rice's theorem.

   (e) The claim is true. Verify that $L_{\Sigma^\star} = \{\langle M\rangle \mid L(M) = \Sigma^\star\} \notin \mathcal{RE} \cup \text{co}-\mathcal{RE}$. Now, we prove $L_{\Sigma^\star} \leq_m L_2$ via the reduction $f(\langle M\rangle) = \langle M'\rangle$, where M' on an input $x = x_1 \dots x_n$:

   - If $x = \epsilon$, reject.
   - Otherwise, simulate M on $x_2 \dots x_n$ and answer accordingly.

   Clearly, f is computable. Now, if $L(M) = \Sigma^\star$ then $L(M') = \Sigma^\star \setminus \{\epsilon\}$, so $\langle M'\rangle \in L_2$. Otherwise, there exists $w \in \Sigma^\star$ such that $w \notin L(M)$. Assume w.l.o.g. that $\Sigma = \{0,1\}$, so M' does not accept $0w, 1w$ and ϵ. Thus, $|\Sigma^\star \setminus L(M')| \geq 3$ and $\langle M'\rangle \notin L_2$.

3. (a) Let M be the TM that decides L in polynomial time. $M^\star$ on $x = x_1 \dots x_n$:

   - Construct a directed graph $G = (V, E)$ where $V = \{1, \dots, n+1\}$ and for every $i < j$, $(i,j) \in E$ if and only if $M(x_{i,\dots,j-1}) = 1$.
   - Check if there exists a path in G from 1 to $n+1$.
   - If such path exists, accept. Otherwise, reject.

   There are $O(n^2)$ possible edges in G, and for every possible edge we simulate M. Then, we run a reachability algorithm (say, BFS). Thus, $M^\star$ runs in polynomial time. If a partition $x = w_1 \dots w_k$ exists such that $w_i \in L$ for every i then there is a path from 1 to $n+1$ in G. Otherwise, there is no path. Overall, $M^\star$ decides $L^\star$ in polynomial time and hence $L^\star \in \mathcal{P}$.

   (b) Let M be the nondeterministic TM that decides L in polynomial time. $M^\star$ on $x = x_1 \dots x_n$:

   - Guess a partition of x to $x = w_1 \dots w_k$ (how?).
   - For every $i \in \{1, \dots, k\}$, simulate $M(w_i)$.

- If all simulations accepted, accept. Otherwise, reject.

The guessing can be done in linear time, and we simulate M at most n times, so $M^\star$ runs in polynomial time. Now, if $x \in L^\star$ there *exists* a partition $x = w_1 \dots w_k$ exists such that $w_i \in L$ for every i, so there exist computation paths (for every such i) through which M accepts. Thus, there is an accepting computation path for $M^\star$. If $x \notin L^\star$ there exists no such partition, and every computation path of $M^\star$ rejects. Hence, $L^\star \in \mathcal{NP}$.

(c) The main idea here – guessing a *cut* in the aforementioned G, and accept iff all of the induced substrings are accepted in M. Formally, Let M be the nondeterministic TM that decides $\bar{L}$ in polynomial time. $M^\star$ on $x = x_1 \dots x_n$:

i. Let $V = \{1, \dots, n+1\}$.
ii. Guess $A \subseteq V$ such that $1 \in A$ and $n+1 \notin A$.
iii. For every $i < j$ such that $i \in A$ and $j \in V \setminus A$, simulate $M(x_i \dots x_{j-1})$.
iv. If M rejected in one of the executions, $M^\star$ rejects.
v. Otherwise, $M^\star$ accepts.

The polynomiality is clear. Now, we prove that $M^\star$ accepts $\overline{L^\star}$.

- If $x \in \overline{L^\star}$ then $x \notin L^\star$ so there is no partition $x = w_1 \dots w_k$ such that $w_i \in L$ for every i. Hence, there exists a cut in G for which every induced word is not in L. Formally, there exists A whereas for every $a < b$ ($a \in A$, $b \in V \setminus A$), $x_a \dots x_{b-1} \notin L$ (as otherwise, we would be able to create such a good partition by starting with $A = \{1\}$ and always choosing the "good" edge). For this A, it always holds that $x_i, \dots x_{j-1} \in \bar{L}$ so there exists an accepting path for M. Thus, there exists an accepting path for $M^\star$.
- If $x \notin \overline{L^\star}$ then $x \in L^\star$ so there is a partition $x = w_1 \dots w_k$ such that $w_i \in L$ for every i. Hence, for every A there exists $a \in A$ and $b \in V \setminus A$ such that $x_a, \dots, x_{b-1} \in L$ (as otherwise, we would have an edge-free cut and no partition can be made). Thus, $x_a, \dots, x_{b-1} \notin L$ so M always rejects, and so does $M^\star$.

4. (a) The claim is true. As B is nontrivial there exist $y \in B$ and $z \notin B$. Set $n_0 = \max\{|y|, |z|\} + 1$ and $f(x)$ to be y if $x \in A$ and z otherwise. As $A \in \mathcal{P}$, f can be computed in polynomial time, and the correctness easily follows. Also, as $|f(x)| < n_0$ for every x satisfying $|x| \geq n_0$, the reduction is also shrinking.

(b) The claim is false. Assume to the contrary that there is a shrinking reduction f from SAT to SAT with a constant n_0. Denote $\mathrm{SAT}_{n_0} = \{\langle\varphi\rangle \in \mathsf{SAT} \mid |\langle\varphi\rangle| \leq n_0\}$. $\mathrm{SAT}_{n_0} \in \mathcal{P}$ as it is finite. Deciding SAT in $\mathcal{P}$ will be as follows: Given φ, compute the series φ_k such that $\varphi_0 = \varphi$ and $\varphi_k = f(\varphi_{k-1})$. The computation stops when we reach a k' such that $|\langle\varphi_{k'}\rangle| \leq n_0$ and we answer according to whether $\varphi_{k'} \in \mathrm{SAT}_{n_0}$ or not. As the reductions preserve correctness, it is easy to see that $\varphi_{k'} \in \mathrm{SAT}_{n_0}$ iff $\varphi \in \mathsf{SAT}$. Also, the above procedure can be done in polynomial time, as f is polynomial and we apply it linear number of times. Therefore, $\mathsf{SAT} \in \mathcal{P}$, in contradiction to $\mathcal{P} \neq \mathcal{NP}$.

5. (a) The claim is true, by the following chain of reductions:

- $\mathsf{CLIQUE} \leq_p \mathsf{VC}$: Given $\langle G, k\rangle$ where $G = (V, E)$, output $\langle \bar{G}, |V| - k\rangle$ where $\bar{G} = (V, E')$ and $\{u, v\} \in E$ iff $\{u, v\} \in E'$. Prove that G has a clique of size k iff $\bar{G}$ has a vertex cover of size $|V| - k$.

- $\mathsf{VC} \leq_p \mathsf{IS}$: Given $\langle G, k\rangle$ where $G = (V, E)$, output $\langle G, |V| - k\rangle$. It is easy to show that G has a vertex cover of size k iff it has an independent set of size $|V| - k$.
- $\mathsf{IS} \leq_p \mathsf{CLIQUE}$: Given $\langle G, k\rangle$, output $\langle \bar{G}, k\rangle$. It is easy to show that G has an independent set of size k iff it has a clique of size k.

Now, it is easy to prove that if $A \leq_p B$ and $B \leq_p C$ then $A \leq_p C$, so we are finished.

(b) The claim is false. If $H_{TM} \leq_p \overline{H_{TM}}$ then $H_{TM} \leq_m \overline{H_{TM}}$ and $H_{TM} \in$ co-$\mathcal{RE}$. As $H_{TM} \in \mathcal{RE}$, $H_{TM} \in \mathcal{RE} \cap$ co-$\mathcal{RE} = \mathcal{R}$, in contradiction.

(c) The claim is false. If SAT $\leq_p \{1\}$ (both languages are in $\mathcal{NP}$) then SAT $\in \mathcal{P}$, in contradiction to $\mathcal{P} \neq \mathcal{NP}$.

6. (a) On input $\langle G\rangle$ where $G = (V, E)$, the reduction is:
   - Choose an arbitrary vertex $v \in V$.
   - Construct $G' = (V', E')$ where $V' = (V \setminus \{v\}) \cup \{v_{in}, v_{out}\}$, and

   $$E' = \{(u_1, u_2) \mid (u_1, u_2) \in E \wedge u_1, u_2 \neq v\} \cup \{(u, v_{in}) \mid (u, v) \in E\} \cup \{(v_{out}, u) \mid (v, u) \in E\}.$$

   - Return $\langle G', v_{out}, v_{in}\rangle$.

   The reduction is obviously polynomial. Now,
   - If G has a Hamiltonian cycle, w.l.o.g. it is of the form $v \to u_1 \to \ldots \to u_k \to v$. Then, in G' there is a Hamiltonian path $v_{out} \to u_1 \to \ldots \to u_k \to v_{in}$.
   - If G' has a Hamiltonian path $v_{out} \to u_1 \to \ldots \to u_k \to v_{in}$ then in G there must be a cycle $v \to u_1 \to \ldots \to u_k \to v$.

   (b) It is trivial that $\mathsf{UnHamPath} \in \mathcal{NP}$. It is then left to show that $\mathsf{HamPath} \leq_p \mathsf{UnHamPath}$. On input $\langle G, s, t\rangle$, the reduction is:
   - Construct an undirected $G' = (V', E')$, where $V' = \bigcup_{v \in V} \{v_{in}, v_{mid}, v_{out}\}$ and

   $$E' = \left(\bigcup_{v \in V} \{\{v_{in}, v_{mid}\}, \{v_{mid}, v_{out}\}\}\right) \cup \{\{u_{out}, v_{in}\} \mid (u, v) \in E\}.$$

   - Return $\langle G', s_{in}, t_{out}\rangle$.

   The reduction is obviously polynomial. Now,
   - If there exists a Hamiltonian path in G, $s \to u_1 \to \ldots \to u_k \to t$, there exists a Hamiltonian path in G',

   $$s_{in} \to s_{mid} \to s_{out} \to (u_1)_{in} \to (u_1)_{mid} \to (u_1)_{out} \to (u_2)_{in} \to \ldots \to t_{in} \to t_{mid} \to t_{out}.$$

   - It is left to show that a Hamiltonian path in G' must go from a triplet of vertices to triplet of vertices. Prove it yourselves.

7. We first prove that:

   - $\mathsf{UpToOneSAT} \in$ co-$\mathcal{NP}$. Consider the language $\overline{\mathsf{UpToOneSAT}}$. It is easy to see that it is in $\mathcal{NP}$, as the witness is simply two distinct satisfying assignments.

- $\overline{\mathsf{UpToOneSAT}} \in \mathcal{NPC}$. We prove that $\mathsf{SAT} \leq_p \overline{\mathsf{UpToOneSAT}}$. Given a CNF φ, the reduction outputs $\varphi' = \varphi \wedge (v \vee \neg v)$ where v is a variable that is not in φ. The fact that the reduction is polynomial is trivial. Now, if φ has a satisfying assignment then φ' has at least two satisfying assignments. If φ is not satisfiable then surely neither is φ'.

Now, we prove $\mathcal{NP} = \text{co}-\mathcal{NP}$ under the assumption that $\mathsf{UpToOneSAT} \in \mathcal{NP}$:

- Let $L \in \mathcal{NP}$. Then, $L \leq_p \overline{\mathsf{UpToOneSAT}}$ and $\bar{L} \leq_p \mathsf{UpToOneSAT}$. As $\mathsf{UpToOneSAT}$ is in $\mathcal{NP}$, $\bar{L} \in \mathcal{NP}$ so $L \in \text{co}-\mathcal{NP}$.
- Let $L \in \text{co-}\mathcal{NP}$. Then, $\bar{L} \in \mathcal{NP}$ and we proved that $\bar{L} \leq_p \overline{\mathsf{UpToOneSAT}}$, so $L \leq_p \mathsf{UpToOneSAT}$. As $\mathsf{UpToOneSAT}$ is in $\mathcal{NP}$, $L \in \mathcal{NP}$.