Assignment 10: PTime reductions and NP-completeness

Solutions

A. For each of the following determine whether it is true, and explain your answer.

(i) If L is NP and $L \leqslant_p L'$ then L' is NP.
Solution. False. Let K be a non-NP language (for example an undecidable language). Take $L' = L \cdot \# \cdot K$. Then $L \leqslant_p L'$. But also $K \leqslant_p L'$, so L' is non-NP.

(ii) If L is NP-hard and $L \leqslant_p L'$ then L' is NP-hard.
Solution. True. If L is NP-hard then (by dfn) every NP-problem is $\leqslant_p L$. By transitivity of $\leqslant_p$, every NP problem is $\leqslant_p L'$.

(iii) If L' is NP-hard and $L \leqslant_p L'$ then L is NP-hard.
Solution. False. The extra assumption implies that there is a PTime-decidable problem $\mathcal{P}$ that is not NP-hard, for otherwise $\mathcal{P}$ would be reducible to any non-trivial problem L' and yet not be NP-hard.

1. (20%) Consider the following decision problems, and the corresponding claims that they are NP. For each claim determine whether it is valid. (If b is a binary string then we write $[b]_2$ for its numeric value as a binary numeral.)

(a) *Given a Turing acceptor M, does it accept some string w within $\leqslant |w|^2$ steps.*
Claim: We can take as PTime certificate for M a string w accepted by M in $\leqslant |w|^2$ steps.

(b) *Given a Turing acceptor M and a binary numeral b,*
M accepts some w of length $\leqslant [b]_2$ in $\leqslant |w|^2$ steps.
Claim: We can take as PTime-certificate for an instance (M, b) a string w accepted by M in $\leqslant |w|^2$ steps.

(c) *Given a Turing acceptor M and a unary numeral I^n,*
M accepts some w of length $\leqslant$ in $\leqslant n^2$ steps
Claim: As PTime-certificate for (M, v) we can take a string w of length $\leqslant n$ accepted by M in $\leqslant |w|^2$ steps.

(d) *Given a Turing acceptor M, does it accept ε.*
Claim: We can take as PTime-certificate for M an accepting trace of M for input ε.

(e) *Given a boolean expression E, is E satisfied by a majority of all valuations for E's variables?*

Claim: We can take as PTime certificate for E a list of valuations that satisfy E.

B. Define **INTEGER-MATCH**: *Given two finite sets S, T of positive integers, are there non-empty subsets $P \subseteq S$ and $Q \subseteq T$ such that $\sum P = \sum Q$.*

Given that **EXACT-SUM** is NP-hard, show that **INTEGER-MATCH** is NP-complete.

Solution. **INTEGER-MATCH** has a PTime certification, with instance (S, T) certified by sets $P \subseteq S$ and $Q \subseteq T$ such that $\sum P = \sum Q$.

The certificate's size is bounded by the size of (S, T) and its correctness can be verified in PTime. So **INTEGER-MATCH** is NP.

To show NP-hardness we define a reduction $\rho :$ **EXACT-SUM** $\leqslant_p$ **INTEGER-MATCH**. ρ maps an instance (S, t) of **EXACT-SUM** to the instance $(S, \{t\})$ of **INTEGER-MATCH**.

ρ is clearly computable in PTime. It is a reduction: If (S, t) satisfies **EXACT-SUM** with a subset P then $(S, \{t\})$ satisfies **INTEGER-MATCH** with the given P and $Q = \{t\}$.

Conversely, if **INTEGER-MATCH** is satisfied with subsets P, Q then $Q = \{t\}$, since Q can't be empty, and so (S, t) satisfies **EXACT-SUM** with that same P.

Given that **EXACT-SUM** is NP-hard, it follows that **INTEGER-MATCH** is NP-hard as well, and since it is NP, **EXACT-SUM** is NP-complete.

2. (20%) **ZERO-SUM**: *Given a finite set S of integers (not necessarily positive), is there a non-empty subset $Z \subseteq S$ that adds up to 0, i.e. $\sum Z = 0$.*

Given that **EXACT-SUM** is NP-hard, prove that **ZERO-SUM** is NP-complete. [Hint: For the reduction from **EXACT-SUM** add to the set one entry.]

Solution. We saw that **ZERO-SUM** is NP. We prove that it is NP-hard by a reduction of **EXACT-SUM** to it.

Let $\rho :$ **EXACT-SUM** $\leqslant_p$ **ZERO-SUM** map instance (S, t) of **EXACT-SUM** to the instance $S \cup \{-t\}$ of **ZERO-SUM**. We have $\sum S = t$ iff $\sum(S \cup \{-t\}) + t = 0$, so this is a reduction. It is trivially P-size, and PTime-computable.

3. (20%) **BISAT**: *Given a boolean expression E, is it satisfied by at least two different valuations.*

Given that **BOOL-SAT** is NP-hard, prove that **BISAT** is NP-complete.

Solution. A certificate for an instance E is a pair of different valuations, each satisfying E. The certificate is of size linear in $|E|$, and can be checked in linear time.

BISAT is NP-hard because BOOL-SAT is NP-hard and $\rho:$ **BOOL-SAT** $\leqslant_p$ **BISAT** where ρ maps an instance $E[x_1 \ldots x_k]$ of BOOL-SAT to the expression $E[x_1 \ldots x_k] \vee E[y_1 \ldots y_k]$, with $y_1 \ldots y_k$ fresh and distinct variables.

ρ is in linear-time trivially.

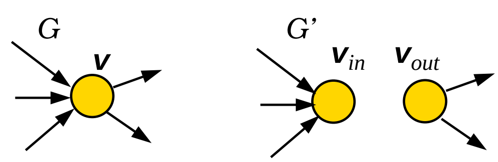
ρ is a reduction: Suppose $E[x_1 \ldots x_k]$ is satisfied by a valuation $V[x_1 \ldots x_k]$; let $V'[\vec{x}]$ be some other valuation over $\vec{x}$. Then $E[\vec{x}] \vee E[\vec{y}]$ is satisfied by the valuation $V[x_1 \ldots x_k] \cup V'[y_1 \ldots y_k]$ as well as by the valuation $V'[x_1 \ldots x_k] \cup V[y_1 \ldots y_k]$. These valuations are different, because we took V' to be different from V .

Conversely, if $E[x_1 \ldots x_k] \vee E[y_1 \ldots y_k]$ is satisfied by a valuation V then one of the disjunct is satisfied by V and so E is satisfiable.

4. Recall that the **HAMILTONIAN-PATH (HP)** problem asks, given a directed graph G , whether it has a Hamiltonian-path (H-path), i.e. a path visiting every vertex once. The **HAMILTONIAN-CYCLE (HC)** problem asks the same question for a ***cycle***, i.e. a closed loop.

(i) Define a reduction $\rho:$ **HC** $\leqslant_p$ **HP**.

Solution. Given a digraph $G=(V,E)$ Chose a vertex $v \in V$. Let $G' = \rho(G)$ be G with v split into two vertices v_{in} and v_{out}. v_{in} inherits the incoming edges of v , and v_{out} the outgoing edges of v .



ρ is computed in PTime trivially.

Suppose G has a H-cycle. $v \to v_1 \cdots \to v_k \to v$.
Then $v_{out} \to v_1 \cdots \to v_k \to v_{in}$ is a H-path in G'.
Conversely, if G' has a H-path then the path's first vertex must be v_{out} (which has no incoming edges) and it must end at v_{in} (which has no outgoing edges). So $v \to v_1 \cdots \to v_k \to v$ is a H-cycle in G .

(a) Define a reduction $\rho:$ **HP** $\leqslant_p$ **HC**.
[Hint: For the reduction add a vertex]

Solution. Let ρ map an instance G of **HP** to the di-graph G' obtained by adding to G a new vertex v , and for each vertex u of G an edge from v to u and an edge from u to v.

ρ is clearly computable in PTime. To show that it is a reduction, assume G has a Hamiltonian path $u_1, \cdots, u_k$. Then $v, u_1, \cdots, u_k, v$ is a Hamiltonian cycle in G' .

Conversely, if there is a Hamiltonian cycle in G', it can be listed starting with v: $v, u_1, \ldots, u_k, v$. Then $u_1, \cdots, u_k$ is a Hamiltonian path in G.

5. (20%) A simple graph $G = (V, E)$ is a ***subgraph*** of $G' = (V', E')$ if $V \subseteq V'$ and there is an injection $j : V \to V'$ that preserves adjacency, i.e. for all $x, y \in V$ we have $x(E)y$ iff $(jx)(E')(jy)$.

SUBGRAPH: *Given simple graphs $G = (V, E)$ and $G' = (V', E')$, is G a subgraph of G'.*

Given that **CLIQUE** is NP-hard, show that **SUBGRAPH** is NP-complete.

Solution. The problem is NP: A certificate for $G = (V, E)$ being a subgraph of $G' = (V', E')$ is an adjacency-preserving injection $j : V \to V'$. Checking that j is an injection and that it is adjacency-preserving can be done in time linear in $|V| + |E|$.

SUBGRAPH is NP-hard because we have $\rho :$ **CLIQUE** $\leqslant_p$ **SUBGRAPH** where ρ maps each instance (G, t) of **CLIQUE** to the instance (K_t, G) of **SUBGRAPH**, where K_t is the complete graph over t vertices. ρ is a reduction, because G has a clique of size $\geqslant t$ iff K_t is a subgraph of G. Moreover, ρ is trivially computed in PTime.

Since **CLIQUE** $\leqslant_p$ **SUBGRAPH** and **CLIQUE** is NP-hard, it folloes that CLIQUE is NP-hard. And since CLIQUE is in NP, we conclude that it is NP-complete.