Hardness HW 1

TAMREF
tamref.yun@snu.ac.kr

Due: September 29, 2022

Rules

- You can just link your former post instead of the solution. Otherwise, it is recommended to write the proof in your language.
- Subproblems are separated for explanatory convenience. You can elaborate the answer for each subproblem, or just provide the whole solution if possible.
- You are qualified if you **read** all the problems, and answered **at least 3** of them. Most easy problems belong to the first page.

Question 1. Integer Program

(a) For $A \in \mathbb{Z}^{N\times M}$ and $b \in \mathbb{Z}^N$, **Zero-One Integer Program** decideds if there is an $x \in \{0,1\}^M$ such that $Ax \geq b$. Prove **SAT** $\leq_p$ **Zero-One Integer Program** to show that it is $\mathbb{NP}-\text{complete}$.

(b) (Optional) If the candidate of $x$is relaxed into $\mathbb{Z}^M_{\geq 0}$, the problem is called **Integer Program (IP)**. What differs in $\mathbb{NP}-\text{complete}$ness of **IP**? Fill the gap to prove it.

Question 2. Pratt's theorem

PRIMES is to test the primality of given integer, the only input.

(a) Show that n is prime if and only if there is an integer g such that $n-1$ is the smallest exponent that $g^{n-1} \equiv 1 \pmod{n}$.

(b) From (a), deduce that n is prime if and only if $g^{(n-1)/q} \not\equiv 1 \pmod{n}$, for every prime divisor q of n.

(c) From (b), provide the polynomial size witness for **PRIMES**.

Question 3. $\mathbb{ZPP} = \mathbb{RP} \cap \text{co}-\mathbb{RP}$

Following the definitions in the slide, prove that $\mathbb{ZPP} = \mathbb{RP} \cap \text{co}-\mathbb{RP}$.

Question 4. Lousy $\mathbb{RP}$ and $\mathbb{BPP}$

For the original definition of $\mathbb{RP}$ and $\mathbb{BPP}$, refer the slide.

(a) Let $\mathbb{RP}_\alpha$ denote the complexity class, where $\Pr[M(x) = \text{yes} \mid x \in A] \geq \alpha$. For all constant $0 < \alpha < 1$, Show that $\mathbb{RP}_\alpha = \mathbb{RP}$.

(b) For $\mathbb{RP}_{1/n^2}$ and $\mathbb{RP}_{1/2^n}$ defined similarly, where n is size of the input, determine whether or not it is equal to $\mathbb{RP}$.

(c) Similarly define $\mathbb{BPP}_\alpha$. For which α we can insist that $\mathbb{BPP}_\alpha = \mathbb{BPP}$?

Question 5. Classic inclusions

Show that $\mathbb{NP} \subseteq \mathbb{PSPACE} \subseteq \mathbb{EXPTIME}$.

Question 6. Diagonal Argument

Assume the following facts.

- Given a TM M, deciding(computing) whether M terminates in polynomial time is **undecidable**.
- Given a TM M and input x, there is a **Universal TM** $\mathcal{U}$ taking the pair (M, x) as input, and simulate $M(x)$ for T discrete steps in $T \log T$ time.
- The set of TMs terminating in $\mathcal{O}(f(n))$ time is **countable** – so we may give them an enumeration.

(a) For $f(n)$ and $g(n)$ such that $f(n) \log f(n) = o(g(n))$, there is a problem could be solved in $\mathcal{O}(g(n))$ time, but never in $\mathcal{O}(f(n))$ time. To show that, Design a TM D terminates in $\mathcal{O}(g(n))$ time, which never could produce identical output with another TM M, terminating in $\mathcal{O}(f(n))$ time. The result is called the **Time Hierarchy Theorem.**

(b) From (a), prove that $\mathbb{P} \neq \mathbb{EXPTIME}$.

Question 7. $\mathbb{BPP} \subseteq \mathbb{PSPACE}$

There's an alternative definition for BPP.

> **Definition.** $A \in \mathbb{BPP}$ if there's a polynomial algorithm M and another polynomial p, takes the original input x attached with the random string $r \in \{0,1\}^{p(|x|)}$, having $\Pr[M(x,r) = \text{yes} \mid x \in A] \geq \frac{3}{4}$ and $\Pr[M(x,r) = \text{no} \mid x \notin A] \geq \frac{3}{4}$.

Relying on the definition, prove that $\mathbb{BPP} \subseteq \mathbb{PSPACE}$. You may try to prove the equivalence of the definition given above, to the definition given in the slide.

Question 8. Equivalence of PH

Recall the oracle definition of PH classes, corrected from the lecture.

- $\Sigma_{i+1} := \mathbb{NP}^{\Sigma_i}$
- $\Pi_{i+1} := \text{co}-\mathbb{NP}^{\Pi_i}$

(a) Prove by induction, that the definition above is equivalent to the definition with alternating quantifiers.

(b) Show that if $\mathbb{P} = \mathbb{NP}$, $P = \Sigma_i$ for all $i \geq 1$.

(c) Show that if $\mathbb{NP} = \text{co}-\mathbb{NP}$, $\mathbb{NP}^{\mathbb{NP}} \subseteq \mathbb{NP}$. (Heavy!)

(d) Assuming (c), show that if $\mathbb{NP} = \text{co}-\mathbb{NP}$, $\Sigma_i = \Pi_i = \mathbb{NP}$ for all $i \geq 1$. This is a tremendous subcase of Polynomial Hierarchy Collapse.

Question 9. Hardness Results from Directed Graph Modeling

These are the class of problems could be solved in similar way. Give a survey to these problems:

(a) Show that the problem **QBF** is $\mathbb{PSPACE}-\text{complete}$.

(b) Show that $\mathbb{NPSPACE} = \mathbb{PSPACE}$. (Savitch's theorem)

(c) $\mathbb{NL}$ is the class of problems could be solved non-deterministically, with $\mathcal{O}(\log n)$ extra r/w memory. Be careful that the 'witness' is bounded in the read-only memory along the input, and it does not really restricted to be logarithmic size. (But bounded by polynomial) Show that the problem *"Given a directed graph G and $s, t \in V(G)$, is there a path from s to t?"* (So called **REACHIBILITY**) is $\mathbb{NL}-\text{complete}$.

(d) From (c), deduce that **2-SAT** is $\mathbb{NL}-\text{complete}$.

Question 10. **2-QBF**

Given a 2-CNF ϕ, the problem $\exists x_1 \forall x_2 \cdots Q_k x_k$ s.t. $\phi(x_1, \cdots, x_k)$ is called **2-QBF**.

Find the linear-time algorithm for **2-QBF**, and solve NERC 2018 Harder Satisfiability. (BOJ 16667)