Computational Complexity

Take-home exam

Hand in via Canvas before Monday June 3, 2024, at 23:59
https://canvas.uva.nl/courses/42595/assignments/496120

Definition 1 ($\mathsf{NP/poly}$)**.** A decision problem $L \subseteq \Sigma^*$ is in the complexity class $\mathsf{NP/poly}$ if there exists:

- polynomials $p, q : \mathbb{N} \to \mathbb{N}$;
- a polynomial-time Turing machine $\mathbb{M}$ (the *verifier*); and
- a sequence $\{\alpha_n\}_{n \in \mathbb{N}}$ with $\alpha_n \in \{0,1\}^{q(n)}$ for each $n \in \mathbb{N}$ (a family of *advice strings*)

such that for every $x \in \Sigma^*$:

$$x \in L \qquad \text{if and only if} \qquad \text{there exists some } u \in \{0,1\}^{p(|x|)} \text{ such that } \mathbb{M}(x, u, \alpha_{|x|}) = 1.$$

One can equivalently define $\mathsf{NP/poly}$ as the class of all decision problems decidable by a polynomial-time nondeterministic Turing machine that has access to a polynomial-length family of advice strings. (You may use either definition (or both) in your solutions.)

Definition 2 ($\mathsf{coNP/poly}$)**.**

$$\mathsf{coNP/poly} = \{\ L \subseteq \Sigma^* \mid \overline{L} = (\Sigma^* \setminus L) \in \mathsf{NP/poly}\ \}.$$

Definition 3 ($\Sigma_i^{\mathrm{p}}/\mathsf{poly}$ and $\Pi_i^{\mathrm{p}}/\mathsf{poly}$)**.** The complexity classes $\Sigma_i^{\mathrm{p}}/\mathsf{poly}$ and $\Pi_i^{\mathrm{p}}/\mathsf{poly}$, for $i \geq 2$, are defined analogously—by taking the definitions of Σ_i^{p} and Π_i^{p} and adding a polynomial-size family of advice strings that the verifier machine is given access to.

Question 1 (*3pts; a: 2pts, b: 1pt*)**.** In this question, you will prove that if $\mathsf{NP} \subseteq \mathsf{coNP/poly}$, then the Polynomial Hierarchy collapses. The general proof line will be as follows.

> You will show that if $\mathsf{NP} \subseteq \mathsf{coNP/poly}$, then $\Sigma_3^{\mathrm{p}} \subseteq \mathsf{NP/poly}$. The following (true) statement, which you do not have to prove, can then be used to show that the Polynomial Hierarchy collapses.
>
> If $\Sigma_3^{\mathrm{p}} \subseteq \mathsf{NP/poly}$, then $\Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$.

Complete the proof by doing the following.

(a) Prove that if $\mathsf{NP} \subseteq \mathsf{coNP/poly}$, then $\Sigma_2^{\mathrm{p}}/\mathsf{poly} \subseteq \mathsf{NP/poly}$.

(b) Prove that if $\mathsf{NP} \subseteq \mathsf{coNP/poly}$, then $\Sigma_3^{\mathrm{p}} \subseteq \mathsf{NP/poly}$.

- *Hint:* use the statement that you proved for **(a)**.

Definition 4. Consider the following problem CLAUSE ENTAILMENT:

> *Input:* A propositional formula φ, and a propositional clause c (i.e., a disjunction of literals).
>
> *Question:* $\varphi \models c$? I.e., is it the case that all truth assignments α that make φ true also make c true?

Definition 5. We say that there is a *hint system* for CLAUSE ENTAILMENT if there exists a computable function $f : \Sigma^* \to \Sigma^*$ (called the *hint function*) and a polynomial-time decidable problem Q such that for each input (φ, c) of CLAUSE ENTAILMENT it holds that $\varphi \models c$ if and only if $(\varphi, f(\varphi), c) \in Q$.

Definition 6. Let $f : \Sigma^* \to \Sigma^*$ be a function. We say that f is *polynomial-size* if there exists a polynomial p such that for all $x \in \Sigma^*$ it holds that $|f(x)| \leq p(|x|)$.

Question 2 (*4pts; a: 1pt, b: 1pt; c: 2pts*).

(a) Prove that the function f_0 that for any propositional formula φ outputs its truth table (over the variables appearing in φ) leads to a hint system for CLAUSE ENTAILMENT. That is, if $f_0(\varphi)$ consists of a list mentioning for each truth assignment $\alpha : \mathrm{Var}(\varphi) \rightarrow \{0,1\}$ whether or not α makes φ true.

In particular, identify a polynomial-time decidable problem Q such that for each formula φ and each clause c it holds that $\varphi \models c$ if and only if $(\varphi, f_0(\varphi), c) \in Q$. Make sure to prove that Q is polynomial-time decidable. You do not have to prove that f_0 is computable.

– *Note:* f_0 is not a polynomial-size function.

(b) Prove that if there is a hint system for CLAUSE ENTAILMENT with a polynomial-time computable hint function f, then $\mathsf{P} = \mathsf{NP}$.

(c) Prove that if there is a hint system for CLAUSE ENTAILMENT with a polynomial-size hint function f, then the Polynomial Hierarchy collapses.

– *Hint:* for different values of $\ell \in \mathbb{N}$, consider the formula:

$$\varphi_\ell = \bigwedge_{1 \leq i \leq (2\ell)^3} (y_i \rightarrow c_i),$$

where $c_1, \dots, c_{(2\ell)^3}$ is an enumeration of all possible clauses of size 3 over the variables $x_1, \dots, x_\ell$.

Definition 7. Consider the following problem SET PACKING:

Input: A finite set U, a set $\mathcal{S} \subseteq \mathcal{P}(U)$ of subsets of U, and a positive integer $k \in \mathbb{N}$ (given in unary).

Question: Are there k sets $S_1, \dots, S_k$ in $\mathcal{S}$ that are pairwise-disjoint—that is, such that $S_i \cap S_{i'} = \emptyset$ for all $1 \leq i < i' \leq k$?

Question 3 (*3pts; a: 1/2pt, b: 1 1/2pts, c: 1pt*).

(a) Prove that there exists an algorithm that solves SET PACKING in time $n^{O(k)}$, where n denotes the size of the input.

(b) Prove that there does not exist an algorithm that solves SET PACKING in time $2^k \cdot n^{o(k)}$, assuming the ETH.

– *Hint:* Consider the following reduction from 3COL to SET PACKING. Let $G = (V, E)$ be an instance of 3COL with $|V| = n$. The reduction partitions the nodes (arbitrarily) into $\log n$ groups $V_1, \dots, V_{\log n}$ consisting each of at most $n/\log n$ nodes.

It then constructs an instance $(U, \mathcal{S}, k)$ of SET PACKING as follows. We set $k = \log n$. The set C consists of all 3-colorings μ that are defined on exactly one of $V_1, \dots, V_{\log n}$ and that do not assign any two nodes connected by an edge in E to the same color. That is, $C = \bigcup_{1 \leq i \leq \log n} C_i$ where C_i is the set of all colorings $\mu : V_i \rightarrow \{1,2,3\}$ such that for no edge $\{u,v\} \in E$ it holds that $u \in V_i$, $v \in V_i$ and $\mu(u) = \mu(v)$. The set U consists of all size-2 sets $\{\mu_1, \mu_2\} \subseteq C$ of colorings in C.

Finally, the set $\mathcal{S}$ is constructed as follows. For each $\mu \in C$, we construct a set $S_\mu \subseteq U$ as follows. Remember that each element of C corresponds to some 3-coloring of a subset of V. Take an arbitrary $\mu \in C$. Then S_μ contains $\{\mu, \mu'\}$ for all colorings $\mu' \neq \mu$ such that either (1) μ and μ' are defined on the same set of nodes, or (2) μ and μ' are defined on different sets of nodes and there is some edge $\{u,v\} \in E$ such that μ and μ' combined assign the same color to both u and v.

– *Note:* you still have to prove that this reduction is correct.

(c) Prove that there does not exist an algorithm that solves SET PACKING in time $2^{2^k} \cdot n^{o(k)}$, assuming the ETH.

– *Note:* for **(c)**, it suffices to indicate where (and how exactly) your solution for **(b)** needs to be adapted.