Problem Set 3

- Due Date: **14th April 2021**
- Turn in your problem sets electronically (pdf or text file) on Acadly.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring to sources other than the text book and class notes is strongly discouraged. But if you do use an external source (eg., other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources (including collaborators) in your writeup. This will not affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.
- The points for each problem are indicated on the side. There are **8 questions** with a total of **100 points** in this problem set.
- Some of the questions are broken-down in to multiple subdivisions to guide you towards a solution. Feel free to use the earlier subdivisions for later ones, even if you haven't solved it (yet).
- Be clear in your writing.

Question 1. Show that $\mathsf{NP} \subseteq \mathsf{P/poly} \implies \mathsf{PH} \subseteq \mathsf{P/poly}$. (7)

Question 2 (Succinct set-cover (Problem 5.11))**.** (8)

The input to the Succinct-Set-Cover problem is a collection of 3-DNFs $\{\varphi_1, \ldots, \varphi_m\}$, each on m variables, and an integer $k > 0$. The computational task is to verify if there is a subset $S \subseteq [m]$ of size at most k such that

$$\bigvee_{i \in S} \varphi_i$$

is a tautology (that is, every $x \in \{0,1\}^n$ is a satisfying assignment for it).

Show that Succinct-Set-Cover $\in \Sigma_2^P$.

Question 3. (2+3+2+3+5)

(i) Consider the following language L corresponding to the encodings of *True* expressions of the form

$$\text{“}(\exists x \in \{0,1\}^m \;\; \varphi(x)) \Leftrightarrow (\forall y \in \{0,1\}^m \;\; \psi(y))''$$

where φ and ψ are some polynomial time computable predicates.

Show that $L \in \mathsf{PH}$. At what level of the hierarchy is it in?

(ii) Let $L \in \mathsf{NP}$ be any language that you are promised is in $\mathsf{P/poly}$. This means that there is a sequence of “advice strings” $\{z_i\}_{i=1}^{\infty}$ and a polynomial time deterministic TM M such that for all x we have $x \in L \Leftrightarrow M(x, z_{|x|}) = 1$.

Define the following language:

$$\text{ValidAdvice}_L = \{(z, n) \;:\; \forall x \in \{0,1\}^n \;\; x \in L \Leftrightarrow M(x, z) = 1\}$$

Show that $\text{ValidAdvice}_L \in \mathsf{PH}$. What level of the hierarchy is it in?

(iii) Try and give a different proof of the Karp-Lipton-Sipser theorem using the above observations.

(iv) Suppose $L \in \mathsf{coNP}$ that is promised to be in $\mathsf{NP/poly}$. Show that $\text{ValidAdvice}_L \in \mathsf{PH}$. What level of the hierarchy is it in?

(v) Show that if $\mathsf{coNP} \subseteq \mathsf{NP/poly}$, then PH collapses. (To what level?)

Question 4. Prove that $\mathsf{coNEXP} \subseteq \mathsf{NEXP/poly}$. (10)

(This is in contrast to the previous problem where you show that it is unlikely that $\mathsf{coNP} \subseteq \mathsf{NP/poly}$)

[Hint: Recall the „advice" used the proof of the Immerman-Szelepcsényi theorem to help an NL machine realise there *no* path of length i from s to t. Is there a similar advice that you can give to an NEXP machine to simulate a coNEXP machine on any input of a certain length?]

Question 5 (Kannan's theorem)**.** (7+8+5)

(i) Fix any constant $c > 0$. Show that there is a language $L \in \mathsf{PH}$ that is not in $\text{SIZE}(n^c)$.

[Hint: Can you try and encode „the lexicographically smallest circuit of size $10n^c$ that is not computable by circuits of size n^c" as a quantified expression?]

(ii) Show that, for any constant $c > 0$, there is a language in $L \in \Sigma_2^P$ that is not in $\text{SIZE}(n^c)$.

[Hint: Either $\mathsf{NP} \subseteq \mathsf{P/poly}$ or not...]

(iii) Note that this means in particular that, for any constant $c > 0$, we know NP is not computable by circuits of size n^c. Why does this not show that $\mathsf{NP} \not\subseteq \mathsf{P/poly}$ (which, if you recall, is stronger than saying $\mathsf{P} \neq \mathsf{NP}$)?

Question 6 (VC Dimension (Problem 5.13))**.** (3+7+10)

The Vapnik-Chervonenkis dimension (VC-dimension) is a very important concept in learning theory. Let $\mathcal{S} = \{S_1, \ldots, S_m\}$ be a collection of subsets of a finite universe U. We shall say that a set $X \subseteq U$ is *shattered* by $\mathcal{S}$ if, for every $X' \subseteq X$, there is some $i \in [m]$ such that $X' = X \cap S_i$.

The VC-dimension of a collection $\mathcal{S}$ is defined as the largest k such that there is some set $X \subseteq U$ of size k that is shattered by $\mathcal{S}$.

Consider the following succinct version of providing the family $\mathcal{S}$ via a Boolean circuit C with $2n$ input bits (which will be encoding a collection $\mathcal{S}$ of 2^n subsets of the universe $U = \{0,1\}^n$):

$$S_i = \{x \in \{0,1\}^n \ : \ C(i,x) = 1\}$$

(where i is provided to the circuit in binary, hence requiring only n bits).

Define the language Circuit-VC-Dim as

$$\text{Circuit-VC-Dim} = \{(C,k) \ : \ C \text{ encodes (as above) a collection of VC-dimension} \geq k\}$$

(i) Show that if $\mathcal{S}$ is the collection encoded (as above) by a Boolean circuit C with $2n$ input bits, then VC-dimension$(\mathcal{S}) \leq n$.

(ii) Show that Circuit-VC-Dim $\in \Sigma_3^P$.

(iii) Show that Circuit-VC-Dim is Σ_3^P complete.

[Hint: It would be convenient to reduce from Σ_3-SAT. Consider an instance $\exists p \forall q \exists r\ \varphi(p,q,r)$ where each of p, q, r are n-bit strings. Let $U = \{0,1\}^n \times [n]$. Try and build a collection $\mathcal{S} = \{S_{pqr} : p,q,r \in \{0,1\}^n\}$ with $S_{pqr} \subseteq \{(p,1),\ldots,(p,n)\}$ that can be encoded by a small circuit. (Observe that the VC-dimension of such a collection cannot be more than n as each set is of size at most n.)

Build this collection so that you can prove $\exists p \forall q \exists r\ \varphi(p,q,r)$ is true if and only if some set of size n (in fact, a set of the form $X = \{(p,1),\ldots,(p,n)\}$) is shattered by this collection. That is,

$$\text{VC-dimension}(\mathcal{S}) \geq n \iff \exists p \forall q \exists r\ \varphi(p,q,r).$$

]

Question 7 (one-sidedness of NP)**.** Show that, if $\mathsf{NP} \subseteq \mathsf{BPP}$, then $\mathsf{NP} = \mathsf{RP}$. (10)

[Hint: You may want to use the downward self-reducibility of SAT]

Question 8 (ZPP (Problem 7.6))**.** (5+5)

(i) Prove that a language L is in ZPP if and only if there is a polynomial time deterministic probabilistic TM M with outputs $\{0,1,?\}$ such that for every $x \in \{0,1\}^*$, with probability 1, we have $M(x) \in \{L(x), ?\}$ and $\Pr[M(x) = ?] \leq 1/2$.

(ii) Show that $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.