Tutorial 07 – Polynomial hierarchy and advice

Exercise 1. *Kannan's Theorem*

A circuit lower bound for the polynomial hierarchy. The aim of this exercise is to show that for each k, there is a language $\mathcal{L}_k \in \Sigma_2^p$ which cannot be computed by circuits of size $O(n^k)$.

1. Show that the result is true if $\mathsf{P/poly} \subsetneq \mathsf{NP}$. Is it equivalent to $\mathsf{P/poly} \subsetneq \mathsf{NP}$?
2. Show that if $\mathsf{NP} \subseteq \mathsf{P/poly}$, then it is enough to prove the claim for some Σ_i^p, $i \geq 2$, instead of Σ_2^p.
3. Show that there are $\leqslant 3^s s^{2s}$ circuits of size s (inputs are in the circuit size, gates are $\wedge, \vee, \neg$, and they are restricted to take at most 2 arguments).
4. Prove that, for sufficiently large n, there are less circuits of size $n^k \lceil \log n \rceil$ than binary words of size n^{k+1}.

Let $x^1, \dots, x^{2^n}$ be the sequence of all words in $\{0,1\}^n$ ordered lexicographically. Given a binary word $a \in \{0,1\}^{n^{k+1}}$ of size n^{k+1} we define a subset $L_a \subset \{0,1\}^n$ as $x^i \in L_a \iff i \leq n^{k+1} \wedge a_i = 1$.

5. Prove that if $a, b \in \{0,1\}^{n^{k+1}}$ are distinct, then $L_a \neq L_b$.
6. Prove that, for sufficiently large n, there exists a such that L_a cannot be recognized by a circuit of size $n^k \lceil \log n \rceil$.
7. Prove that L_a can be recognized by a circuit of size Kn^{k+2} for some $K > 0$.

For every n let $\mathcal{C}_n$ be the set of circuits of size Kn^{k+2} that recognize functions which cannot be recognized by circuits of size $n^k \lceil \log n \rceil$. The previous parts show that $\mathcal{C}_n$ is nonempty for sufficiently large n. For every such n let $C_n \in \mathcal{C}_n$ be the circuit whose binary description is the smallest in the lexicographic order of $\{0,1\}^*$. Define $\mathcal{L}_k$ as $x \in \mathcal{L}_k \iff C_{|x|}(x) = 1$.

8. Prove that $\mathcal{L}_k$ belongs to Σ_i^p for some $i \geq 2$ but it cannot be recognized by circuits of size $O(n^k)$. (Note: $i = 4$ is enough.)
9. Conclude (Hint: Use Karp-Lipton Theorem)

Exercise 2. *Polynomial Hierarchy*

You have seen during the course the quantifier definition of the polynomial hierarchy: $L \in \Sigma_i^p$ if there exists a polytime TM M and a polynomial q such that:

$$x \in L \iff \exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} \dots Q_i u_i \in \{0,1\}^{q(|x|)} M(x, u_1, u_2, \dots, u_i) = 1\,.$$

You have also seen an alternative definition using oracles:

$$\begin{cases} \Sigma_0^p & = \mathsf{P} \\ \Sigma_{i+1}^p & = \mathsf{NP}^{\Sigma_i^p} \end{cases}$$

With PH being defined as $\bigcup_{i \geqslant 0} \Sigma_i^p$.

1. Prove the equivalence between the quantifier-based definition and the oracle-based definition.
2. Give an oracle-based definition for Π_i^p.
3. Show that Σ_i^p is closed under polynomial-time many-one reduction.
4. Show that if there exist a PH-complete problem, then the polynomial hierarchy collapses.
5. Show that if $\Sigma_i^p = \Sigma_{i+1}^p$, then $\mathsf{PH} = \Sigma_i^p$.
6. Propose a family of problems (S_i) such that S_i is Σ_i^p-complete.

Exercise 3. $\mathsf{NP}^{\mathsf{NP}}$

Let MinDNF denote the languages of all tuples (ϕ, k) such that ϕ is a SAT formula in disjunctive normal form, and $k \in \mathbb{N}$ is such that there exists an equivalent formula ϕ' of encoding size $\|\phi'\| \leq k$. More formally,

$$\textsc{MinDNF} = \{(\phi, k) \in \mathsf{DNF} \times \mathbb{N} \colon \exists \phi', \|\phi'\| \leqslant k, \forall x, \phi(x) = \phi'(x)\}\,.$$

Show that $\textsc{MinDNF} \in \mathsf{NP}^{\mathsf{NP}}$.

Exercise 4. *Advice*

1. Prove that $\mathsf{NP} \subseteq \mathsf{P}/\log$ implies $\mathsf{P} = \mathsf{NP}$.
2. Prove that every language $\mathcal{L} \subset \Sigma^*$ belongs to $\mathsf{P}/|\Sigma|^n$.
3. Show that there exists a *decidable* unary language that does not belong to P.
   A language $L \subseteq \{0,1\}^*$ is called sparse if there exists a polynomial p such that $|L \cap \{0,1\}^n| \leqslant p(n)$ for all n
4. Show that every sparse language is in P/poly