Homework 2 (40 points total)

Due on Friday, 10:20 am, 5 May 2023 (112/05/05)

Question 1 (6 points). Prove that the algorithm No-path, procedure Count-Vertex$_G$ and procedure Verify$_G$ in the appendix in Note 4 are all correct. That is, they all compute according to the described task. Argue that they all use only logarithmic space.

Question 2 (3 point). Consider the problem CIRCUIT-EVAL and Theorem 5.5 in Note 5. The main idea for the proof of hardness is as follows. Let $\mathcal{M}$ be a polynomial time DTM. On input word w, the reduction constructs a circuit C such that:

$$C(w) = 1 \qquad \text{if and only if} \qquad \mathcal{M} \text{ accepts } w$$

The construction of C is similar to Cook-Levin reduction for the proof of **NP**-hardness of SAT. Explain why we need the fact that $\mathcal{M}$ is DTM and *not* NTM in the proof of Theorem 5.5.

Question 3 (6 points). Prove that **PH** collapses if any one of the following is true.

- $\mathbf{\Sigma}_i^p = \mathbf{\Pi}_i^p$ for some $i \geqslant 1$.
- There is **PH**-complete language.
- **PH** = **PSPACE**.

Question 4 (4 points). Suppose that A is a language such that $\mathbf{P}^A = \mathbf{NP}^A$. Prove that $\mathbf{PH}^A \subseteq \mathbf{P}^A$.

Question 5 (6 point). Prove Lemmas 6.10 and 6.11 in Note 6.

Question 6. (See Appendix B for the definition of the class size(n^k))

(a) (3 points) Show that every function $f : \{0,1\}^t \to \{0,1\}$ can be computed by a circuit of size $\leqslant 3t2^t$.

(b) (4 points) Show that for every $k \geqslant 1$, there is a language L such that the following holds.

(P1) $L \in \text{size}(n^{k+1})$.

(P2) For sufficiently large n, there is no circuit of size $\leqslant n^k$ that computes $L \cap \{0,1\}^n$.

Conclude that for every $k \geqslant 1$, $\text{size}(n^k) \subsetneq \text{size}(n^{k+1})$.

(c) (4 points) Prove that for every $k \geqslant 1$, there is a language $L \in \mathbf{\Sigma}_4^p$ that has properties (P1) and (P2) above. Then, conclude that for every $k \geqslant 1$, $\mathbf{\Sigma}_4^p \setminus \text{size}(n^k) \neq \emptyset$.

(d) (4 points) Prove that for every $k \geqslant 1$, there is a language $L \in \mathbf{\Sigma}_2^p \setminus \text{size}(n^k)$.

Hint for (b): We know that for every t, there is a function $f : \{0,1\}^t \to \{0,1\}$ such that f is not computable by circuit of size $2^t/(10t)$. Combine this with (a) for some appropriate value t.

Hint for (c): Consider the language L in Question 1. Then, for every n, consider the "lexicographically first" circuit C_n of size $\leqslant n^{k+1}$ that is not equivalent to any of the circuit of size $\leqslant n^k$.

A The definition needed in Question 4

Def: A language L is in the class $\mathbf{\Sigma}_i^p$ *with oracle access to* A, if there is a polynomial $q(n)$ and a polynomial time DTM $\mathcal{M}^A$ such that for every $w \in \Sigma^*$ the following holds.

$$w \in L \quad \text{iff} \quad \exists y_1 \in \{0,1\}^{q(|w|)} \; \forall y_2 \in \{0,1\}^{q(|w|)} \; \cdots \; Qy_i \in \{0,1\}^{q(|w|)} \; \mathcal{M}^A \text{ accepts } (w, y_1, \ldots, y_i)$$

As before, $\mathcal{M}^A$ denotes the TM $\mathcal{M}$ with oracle access to A. A language L is in $\mathbf{PH}^A$, if there is an index i such that L is in the class $\mathbf{\Sigma}_i^p$ with oracle access to A.

B The notation used in Question 6

For a function $g : \mathbb{N} \to \mathbb{N}$, let $\textsc{size}(g)$ denote the class of languages such that $L \in \textsc{size}(g)$ if and only if L is decided by a circuit family $\{C_n\}$ such that for sufficiently large n:

$$|C_n| \quad \leqslant \quad g(n)$$

That is, there is n' such that for every $n \geqslant n'$, $|C_n| \leqslant g(n)$.