Homework 3

Due on Tuesday, 11:59 am, 30 May 2022 (111/05/30)

Note: There are 8 questions altogether. For Questions 1–3, we will use the following notation. 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 $n \geqslant n'$, $|C_n| \leqslant g(n)$.

Question 1.

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

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

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

(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 $k \geqslant 1$, $\textsc{size}(n^k) \subsetneq \textsc{size}(n^{k+1})$.

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.

Question 2. 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 $k \geqslant 1$, $\mathbf{\Sigma}_4^p \setminus \textsc{size}(n^k) \neq \emptyset$.

Hint: 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 $\leqslant n^k$.

Question 3. Prove that for every $k \geqslant 1$, there is a language $L \in \mathbf{\Sigma}_2^p \setminus \textsc{size}(n^k)$.

Question 4.

- Let $\mathcal{H}_{n,k}$ be a pairwise independent collection of hash functions $h : \{0,1\}^{\to}\{0,1\}^k$. Prove that for every $x \in \{0,1\}^n$, for every $y \in \{0,1\}^k$, $\mathbf{Pr}_{h \in \mathcal{H}_{n,k}}[\ h(x) = y\ ] = 2^{-k}$.

- Prove Theorem 8.9, i.e., the collection $\mathcal{H}_{n,n} \stackrel{\mathsf{def}}{=} \{h_{A,b} : A \in \{0,1\}^{n \times n} \text{ and } b \in \{0,1\}^{n \times 1}\}$ is pair-wise independent.

Question 5. Prove that $\mathbf{MA} \subseteq \mathbf{\Sigma}_2^p$.